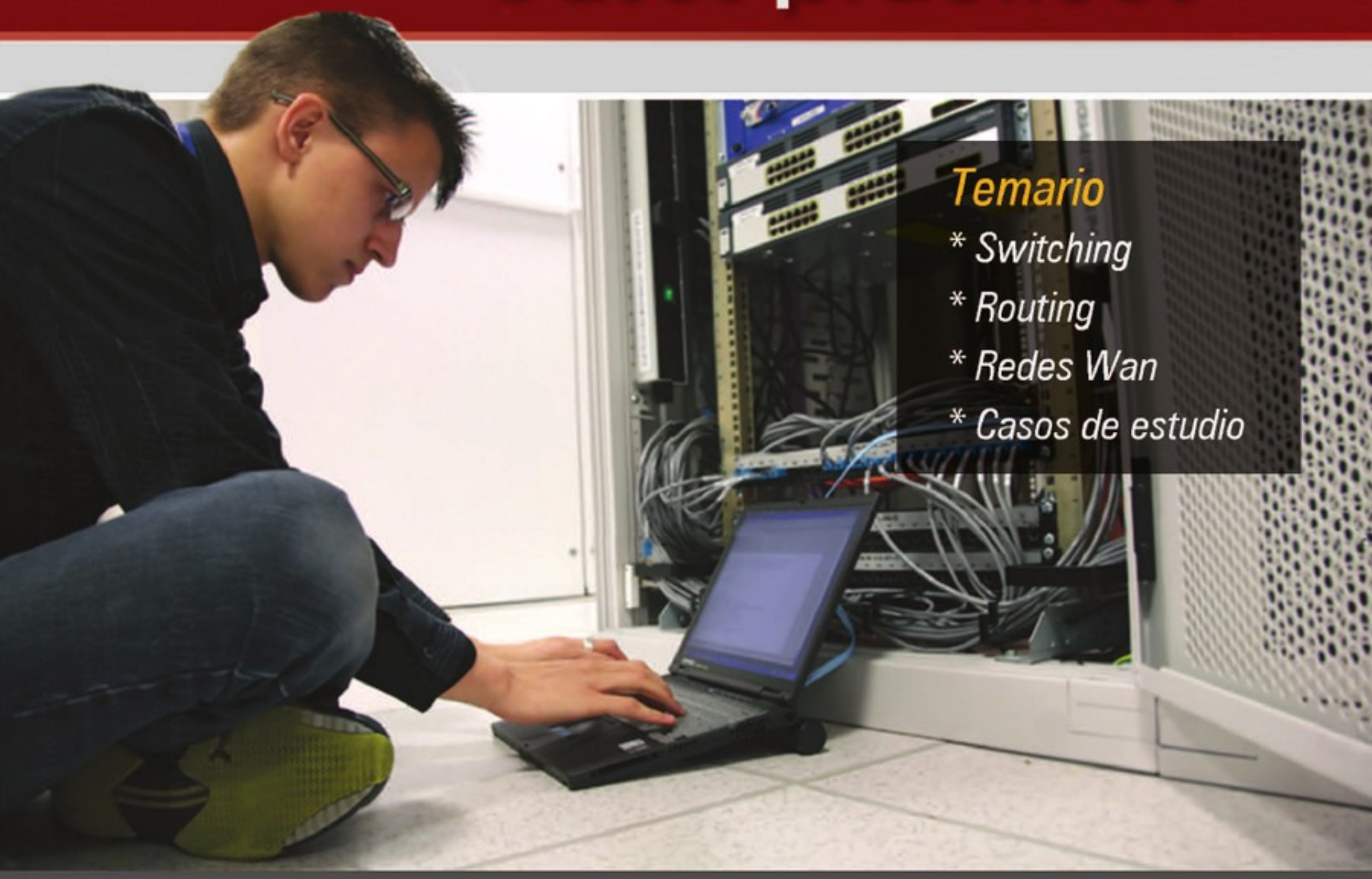
Héctor H. Delgado Ortiz

CCNA Exploration

Casos prácticos



Temario

* *Switching*
* *Routing*
* *Redes Wan*
* *Casos de estudio*

EDITORIAL MACRO®

CCNA Exploration

Casos Prácticos

EMPRESA EDITORA MACRO®

CCNA
Autor: Héctor H. Delgado Ortíz

© Derecho de autor reservado
Empresa Editora Macro E.I.R.L.

© Derecho de edición, arte gráfico y diagramación reservados
Empresa Editora Macro E.I.R.L.

Edición a cargo de:
Empresa Editora Macro E.I.R.L.
Av. Paseo de la República 5613 – Miraflores
Lima - Perú
(511) 719-9700
ventas@editorialmacro.com
http://www.editorialmacro.com

Primera edición: Octubre 2009 - 1000 ejemplares

Impreso en los Talleres Gráficos de
Empresa Editora Macro E.I.R.L.
Lima - Perú

ISBN Nº 978-612-4034-36-7
Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2009-12761

Prohibida la reproducción parcial o total, por cualquier medio o método de este libro sin previa autorización de la Empresa Editora Macro E.I.R.L.

Dedicatoria

"A mi querido hijo, Héctor Fabrizio, a quien un 12 de abril tuve la dicha de ver nacer, por hacerme entender lo necesario que es compartir con los hijos".

Prólogo

Dentro de los capítulos se presenta el desarrollo práctico de la currícula para la certificación CCNA, además de ciertos casos sobre temas de configuración avanzada, con cuya explicación se facilita su entendimiento y aplicación. Así mismo, dichos temas permiten tener un panorama más amplio del entorno de red donde se trabaja y adaptarse a nuevos contenidos.

Se ha desarrollado en una estructura de cuatro capítulos, los cuales se describen a continuación:

Capítulo 1: SWITCHING

Describe el proceso de conmutación de una red LAN, mediante la configuración del switch Catalyst capa 2, el cual está dirigido a operar como punto de distribución y de acceso en el modelo jerárquico de las topologías LAN. Se presentan seis laboratorios en los que se muestra la operación de los switches, indicando su secuencia de carga, la recuperación del IOS y los problemas que se presentan; el funcionamiento conmutado de los dominios de broadcast y su segmentación; el diseño de VLAN en el dominio VTP; la configuración del protocolo STP y sus alternativas de prioridad; así como lo que respecta a la seguridad de puerto y la comunicación entre VLAN.

Capítulo 2: ROUTING

Refiere el mecanismo de operación en los routers, el cual ha sido desarrollado en doce laboratorios donde adicionalmente se presentan casos para modificar la configuración planteada, con su respectiva solución. El contenido describe la configuración básica de los routers, el respaldo y restablecimiento del archivo de configuración y sistema operativo (IOS), la implementación de las diferentes características en el enrutamiento estático, el enrutamiento con los protocolos OSPF, RIP y EIGRP, así como también el diagnóstico de conexiones y la solución de problemas.

Capítulo 3: REDES WAN

Corresponde a la configuración de soluciones que presentan los proveedores de servicio y las alternativas de seguridad en un ambiente de área local y área amplia. Dividido en seis laboratorios donde se profundiza en el trabajo de la tecnología Frame Relay para entender el comportamiento de los protocolos de enrutamiento OSPF y EIGRP, dada su arquitectura NBMA, los tipos de encapsulamiento (HDLC, PPP) y su autenticación, así como también las alternativas en conjunto del servicio de traducción de direcciones (NAT estático, NAT dinámico y NAT de sobrecarga).

Capítulo 4: CASOS DE ESTUDIO

Integra los diversos temas que se presentan en los capítulos anteriores, sumándose la configuración de temas como el servicio DHCP local y remoto, seguridad mediante las listas de control de acceso, autenticación local para el acceso por terminal virtual, configuración del servidor TACACS+, tanto para ambientes inalámbricos como para redes LAN y WAN. El desarrollo comprende nueve casos de estudio que permiten entender el trabajo en conjunto de las diferentes tecnologías, protocolos, servicios y dispositivos de red, así como diferenciar la solución que se brinda a una empresa de acuerdo a sus requerimientos.

Capítulo 5: ANEXOS

Se presentan documentos de información complementaria que amplían los diversos temas descritos en cada capítulo. Puede decirse que se trata de herramientas de utilidad, pues son explicaciones, síntesis de configuración y consejos para facilitar el proceso de aprendizaje de la configuración e implementación de las topologías con equipos Cisco.

Introducción

Las certificaciones internacionales son requerimientos ineludibles para los profesionales en tecnologías de la información, ello explica la importancia de su preparación en el área que uno desarrolla. En la actualidad, se trata de una necesidad que exige estar preparados con habilidades y destrezas, a fin de alcanzar altos niveles de conocimiento en un mercado global altamente competitivo.

La certificación de CCNA, otorgada por Cisco, comprende una visión global para capacitar a los profesionales de networking, facilitando el entendimiento en la instalación, configuración y fusión de redes LAN, redes WAN y servicios de acceso dial para redes pequeñas, incluyendo las tecnologías y protocolos como IP, EIGRP, OSPF, Frame Relay, VLAN, VTP, STP, Ethernet y Listas de Control de Acceso (ACL).

La preparación en la certificación CCNA implica asumir un reto desarrollando actitudes que faciliten el aprendizaje en las diversas áreas del diseño e implementación de las redes mencionadas.

Casos Prácticos de CCNA es un manual de laboratorio que brinda a quien lo desarrolla todas las habilidades y destrezas de un profesional CCNA. Se debe considerar como un complemento al nivel de conocimiento que la certificación permite.

Es un compendio de casos para redes con arquitectura Cisco, planteados de acuerdo a una estructura metodológica que facilita su entendimiento, desarrollándose temas como la implementación de redes conmutadas, el enrutamiento dinámico y estático, las soluciones para redes WAN, así como también la seguridad mediante las listas de control de acceso, entre otros.

El contenido ha sido elaborado en base a cuantiosas experiencias en el trabajo de campo y en el aula, donde se presentan laboratorios que agrupan técnicas para trabajar con diversos temas, explicándose detalladamente su implementación y sintetizando la base teórica, asumiendo su conocimiento por parte del usuario.

El material que se facilita permite el aprendizaje en niveles intermedios y avanzados de networking; puede ser empleado por profesionales o estudiantes de redes, especialistas, y público en general, con la finalidad de certificarse, brindar soluciones, prepararse para la instrucción o enseñanza, estudiar la certificación CCNA, prepararse para estudiar la certificación CCNP, etc.

CONTENIDO

Capitulo 1: Switching

LABORATORIO 1 – SWITCH (Redes conmutadas) 17
DESCRIPCIÓN 17
OBJETIVOS 17
PLANTEAMIENTO 17
LABORATORIO 2 - CARGA DEL SWITCH 22
DESCRIPCIÓN 22
OBJETIVOS 22
PLANTEAMIENTO 22
LABORATORIO 3 - DETERMINANDO CARACTERÍSTICAS EN LOS SWITCHES 26
DESCRIPCIÓN 26
OBJETIVOS 26
PLANTEAMIENTO 26
LABORATORIO N° 4 - IMPLEMENTACION DE VLAN EN UN DOMINIO VTP 32
DESCRIPCIÓN 32
OBJETIVOS 32
PLANTEAMIENTO 32
SOLUCIÓN 33
CONFIGURACION FINAL 36
LABORATORIO N° 5 - IMPLEMENTACIÓN DE VLAN, CON UN DOMINIO VTP Y STP 42
DESCRIPCIÓN 42
OBJETIVOS 42
PLANTEAMIENTO 42
SOLUCIÓN 43
CONFIGURACIÓN FINAL 49
LABORATORIO N° 6 - IMPLEMENTACION DE INTERVLAN 63
DESCRIPCIÓN 63
OBJETIVOS 63
PLANTEAMIENTO 63
SOLUCIÓN 64
CONFIGURACIÓN FINAL DE CADA EQUIPO 67

Capitulo 2: Routing

LABORATORIO Nº 1 - Instalación del IOS en el router 83
DESCRIPCIÓN 83
OBJETIVOS 83
PLANTEAMIENTO 83
Descarga del IOS mediante el puerto LAN para conexión hacia un servidor TFTP 86
LABORATORIO Nº 2 - CONFIGURACIÓN BÁSICA DEL ROUTER 88
DESCRIPCIÓN 88
OBJETIVOS 88
PLANTEAMIENTO 88
LABORATORIO Nº 3 - Diagnóstico de conexiones I 94
DESCRIPCIÓN 94
OBJETIVOS 94
DESCRIPCIÓN 94
DESARROLLO 94
LABORATORIO Nº 4 - Diagnóstico de conexiones II 105
DESCRIPCIÓN 105
OBJETIVOS 105
PLANTEAMIENTO 105
DESARROLLO 105
LABORATORIO N° 5 - RIP Y LAS RUTAS DE RESPALDO 112
DESCRIPCIÓN 112
OBJETIVOS 112
PLANTEAMIENTO 112
DESARROLLO 113
LABORATORIO N° 6 - Redistribución de rutas estáticas en RIP 123
DESCRIPCIÓN 123
OBJETIVOS 123
PLANTEAMIENTO 123
LABORATORIO N° 7 - EIGRP con rutas de distinto ancho de banda 135
INTRODUCCIÓN 135
OBJETIVOS 135
DESCRIPCIÓN 135
DESARROLLO 135

LABORATORIO N° 8 - EIGRP (análisis de DUAL) 144
DESCRIPCIÓN 144
OBJETIVOS 144
PLANTEAMIENTO 144
DESARROLLO 144
LABORATORIO N° 9 - EIGRP y redistribución de rutas estáticas 153
DESCRIPCIÓN 153
OBJETIVOS 153
PLANTEAMIENTO 153
DESARROLLO 154
LABORATORIO N° 10 - OSPF 166
DESCRIPCIÓN 166
OBJETIVOS 166
PLANTEAMIENTO 166
DESARROLLO 167
LABORATORIO N° 11 - OSPF - OPCIONES AVANZADAS 178
INTRODUCCIÓN 178
OBJETIVOS 178
DESCRIPCIÓN 178
TAREAS 187
LABORATORIO N° 12 - Enrutamiento OSPF con rutas por defecto 188
INTRODUCCIÓN 188
OBJETIVOS 188
DESCRIPCIÓN 188
DESARROLLO 188

Capitulo 3: Redes Wan

LABORATORIO N° 1 - PPP y RIP v2 195
INTRODUCCIÓN 195
OBJETIVOS 195
DESCRIPCIÓN 195
DESARROLLO 196
TAREAS 203

LABORATORIO N° 2 - DHCP y NAT 204
INTRODUCCIÓN 204
OBJETIVOS 204
PROCEDIMIENTO 204
LABORATORIO N° 3 - NAT ESTÁTICO Y DE SOBRECARGA 209
INTRODUCCIÓN 209
OBJETIVOS 209
DESCRIPCIÓN 209
DESARROLLO 210
LABORATORIO N° 4 - TOPOLOGÍA HUB AND SPOKE CON SPLIT HORIZON 217
INTRODUCCIÓN 217
OBJETIVOS 217
PROCEDIMIENTO 217
DESARROLLO 217
TAREA 226
LABORATORIO N° 5 - Topología NBMA 228
INTRODUCCIÓN 228
OBJETIVOS 228
DESCRIPCIÓN 228
DESARROLLO 228
LABORATORIO N° 6 - Topologías Multipunto 242
INTRODUCCIÓN 242
OBJETIVOS 242
DESCRIPCIÓN 242
DESARROLLO: 243

Capitulo 4: Casos de Estudio

LABORATORIO N° 1 253
DESCRIPCIÓN 253
OBJETIVOS 253
PLANTEAMIENTO 253
DESARROLLO 254
TAREAS 265

LABORATORIO N° 2 266
INTRODUCCIÓN 266
OBJETIVO 266
DESCRIPCIÓN 266
TAREAS 290
LABORATORIO N° 3 - VLAN CON ENRUTAMIENTO DINÁMICO DE DOS PROTOCOLOS POR CONEXIÓN FRAME RELAY 291
INTRODUCCIÓN 291
OBJETIVOS 291
DESCRIPCIÓN 291
LABORATORIO N° 4 - REDISTRIBUCIÓN DE RUTAS 302
INTRODUCCIÓN 302
OBJETIVO 302
DESCRIPCIÓN 302
DESARROLLO 302
TAREAS 313
LABORATORIO N° 5 - SWITCHING y ROUTING 314
INTRODUCCIÓN 314
OBJETIVOS 314
DESCRIPCIÓN 314
DESARROLLO 315
DIAGNÓSTICO DE ENRUTAMIENTO 325
TAREAS 337
LABORATORIO N° 6 - LISTAS DE CONTROL DE ACCESO 338
DESCRIPCIÓN 338
OBJETIVOS 338
DESCRIPCIÓN 338
DESARROLLO 339
LABORATORIO N° 7 - CONEXIÓN DE VLAN INALÁMBRICA Y EL PUENTE COMO RUTA DE RESPALDO.. 347
INTRODUCCIÓN 347
OBJETIVOS 347
DESCRIPCIÓN 347
DESARROLLO 348
LABORATORIO N° 8 367
INTRODUCCIÓN 367

OBJETIVO 367
DESCRIPCIÓN 367
DESARROLLO 368
TAREAS 381
LABORATORIO N° 9 - Principios básicos de conmutación y enrutamiento intermedio 382
INTRODUCCIÓN 382
OBJETIVO 382
DESCRIPCIÓN GENERAL 382
DESARROLLO 383

Capitulo 5: Anexos

I. LAS "LÍNEAS" DE LOS ROUTERS CISCO 411
II. CONFIGURACIÓN RECOMENDADA 414
III. EL REGISTRO DE CONFIGURACIÓN 420
IV. SOLUCIÓN DE PROBLEMAS BÁSICOS 421
V. COMANDOS DE VERIFICACIÓN 424
VI. SEGURIDAD BÁSICA 427
VII. LISTA DE COMANDOS 433
VIII. SOFTWARE 440

BIBLIOGRAFÍA 447

SWITCHING

La implementación de redes conmutadas permite establecer seguridad, escalabilidad, compatibilidad y disponibilidad de la red, por lo que el proceso de conmutación en una red LAN es necesario. Se han planteado y desarrollado seis laboratorios que describen la operación de los switches Catalyst de capa 2, como se describe a continuación:

LABORATORIO N° 1: REDES CONMUTADAS

Se describe la implementación de varios esquemas tanto para una red plana como para una red conmutada, donde se explica las características de funcionamiento de la red Ethernet, diferenciando su operación en los dominios de colisión y dominios de broadcast, la transmisión full duplex y half duplex, y la identificación de éstas.

LABORATORIO N° 2: CARGA DEL SWITCH

Se explica el proceso e identificación de la secuencia de carga que realiza el sistema operativo en un switch, junto con su configuración inicial adecuada, así como la rutina de eliminar cualquier configuración anterior y el restablecimiento de imágenes IOS.

LABORATORIO N° 3: DETERMINANDO CARACTERÍSTICAS EN LOS SWITCHES

El laboratorio permite revisar criterios básicos de implementación en las opciones de configuración, como el nombre del equipo, contraseñas y el direccionamiento IP. Así también se exponen las características de diagnóstico para equipos vecinos en la implementación tipo malla de una red LAN.

LABORATORIO N° 4: IMPLEMENTACIÓN DE VLAN EN UN DOMINIO VTP

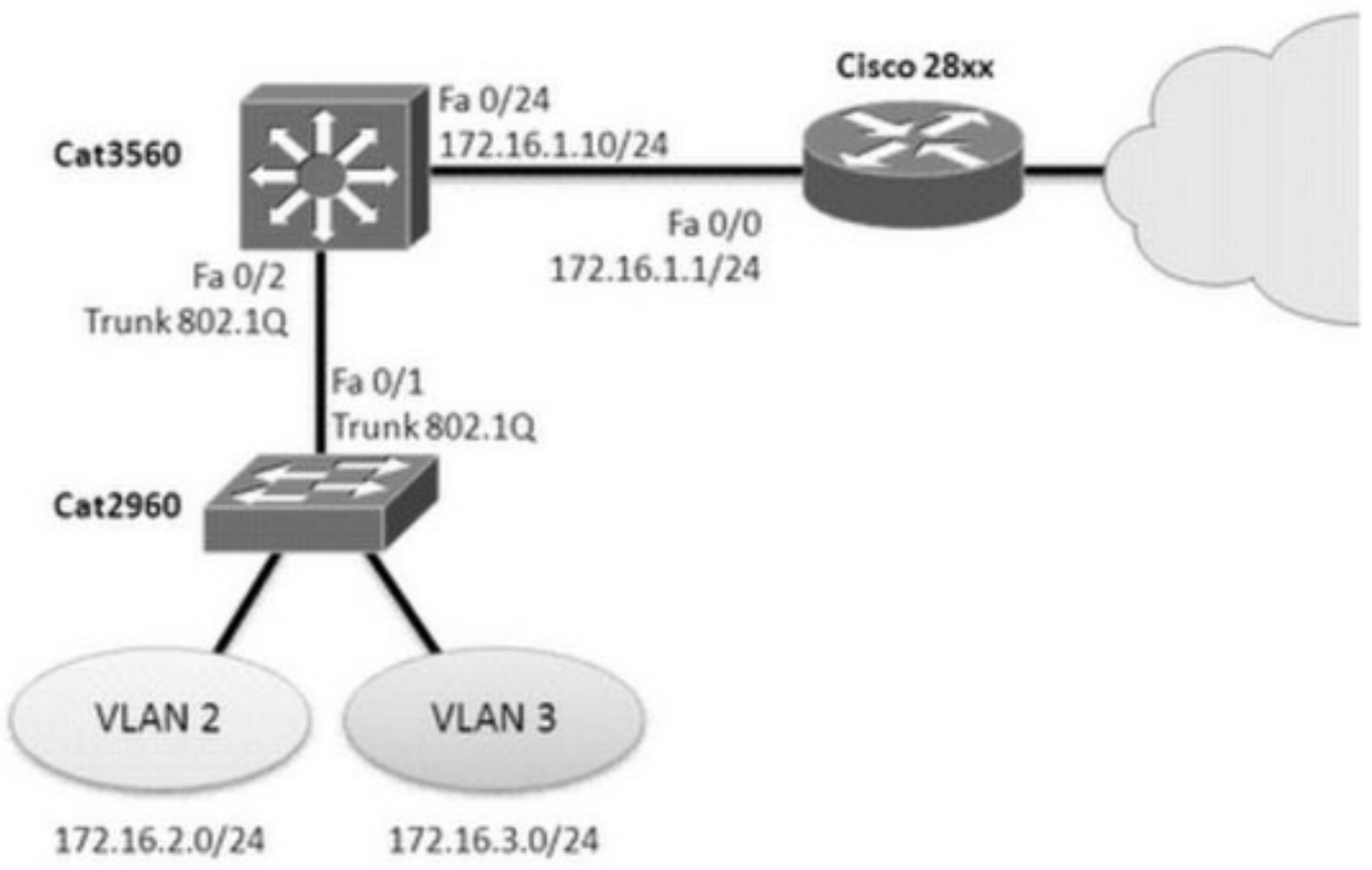
Se detalla el establecimiento de una LAN con redes virtuales en un dominio VTP, permitiendo identificar los elementos necesarios del dominio mediante un esquema cliente-servidor y sus opciones de seguridad. Se trabaja con los tres modos de configuración que permite el protocolo VTP, como son: CLIENT, SERVER y TRANSPARENT.

LABORATORIO N° 5: IMPLEMENTACIÓN DEL DOMINIO VTP Y STP

El funcionamiento de las rutas redundantes es detallado en este laboratorio, dentro de un esquema de dominio VTP y administradas mediante el protocolo spanning tree, donde se configuran los elementos para el funcionamiento y los criterios para optimizar la red, como la elección del Root primary y Root secondary, la prioridad por puertos al elegir un enlace, entre otras cosas.

LABORATORIO N° 6: IMPLEMENTACIÓN DE INTERVLAN

La comunicación entre las subredes que se establecen con la VLAN es facilitada mediante un dispositivo capa 3, que para el presente laboratorio se ha implementado con un router, dentro de un dominio VTP y cierta configuración del protocolo spanning tree. Se muestra la configuración de subinterfaces y se establecen dos enlaces troncales desde el router, variándose la alternativa de un solo enlace y permitiendo equilibrar el tráfico por cada interfaz.


Cisco 28xx
Cat3560
Fa 0/24
172.16.1.10/24
Fa 0/0
172.16.1.1/24
Fa 0/2
Trunk 802.1Q
Fa 0/1
Trunk 802.1Q
Cat2960
VLAN 2
VLAN 3
172.16.2.0/24
172.16.3.0/24

Capítulo

1 Switching

LABORATORIO 1 – SWITCH (Redes conmutadas)

DESCRIPCIÓN

A través de la implementación de redes conmutadas se permite la mejor seguridad, escalabilidad, entre otras características de la red, considerando una serie de aspectos como la segmentación, el establecimiento de VLAN, etc.

Si se va a realizar el estudio de la implementación de redes conmutadas, se debe tener en claro cómo funciona actualmente una red Ethernet, diferenciando las características de funcionamiento en uno y varios dominios de colisión con sus características de operación, así como también, el dominio de broadcast.

OBJETIVOS

- Reconocer la red bajo una implementación de dominio de colisión.
- Diferenciar la operación de transmisión full duplex y half duplex.
- Identificar diferencias entre los dominios de colisión y dominios de broadcast.

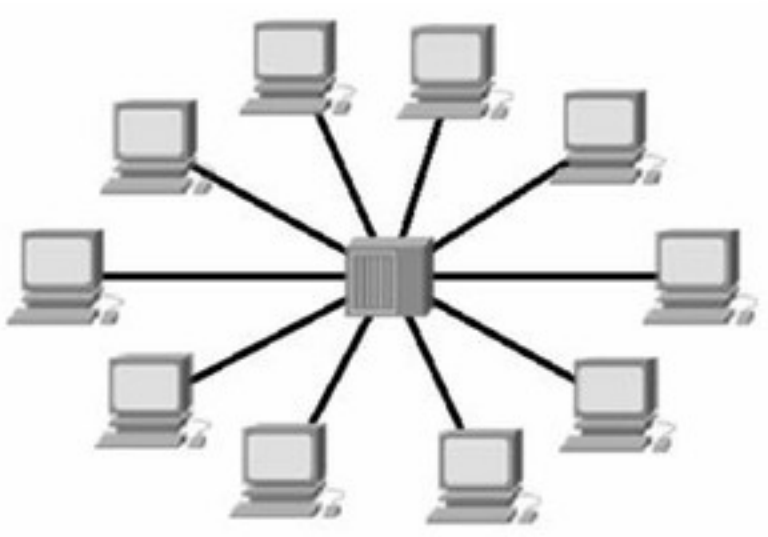
PLANTEAMIENTO

FASE I:

Para la implementación de la redes se podrá emplear cualquier simulador que facilite su operación.

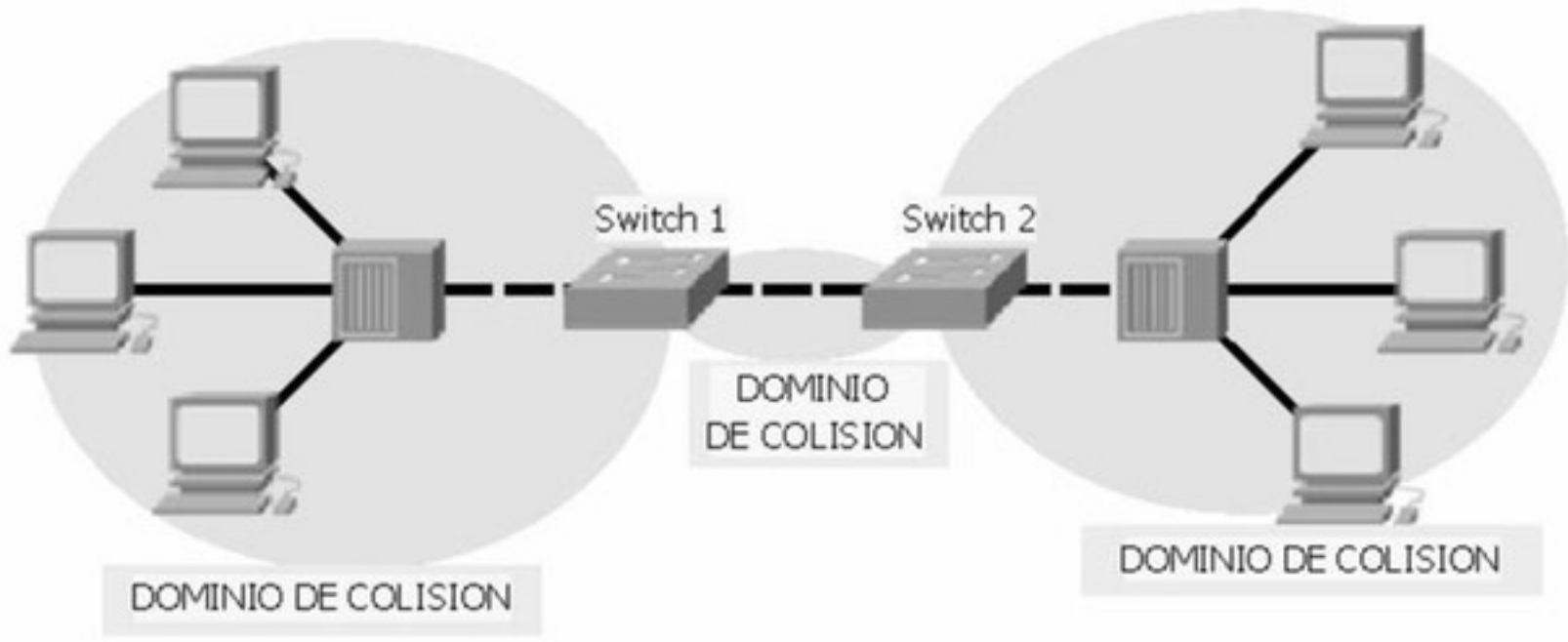
***Nota**: Indicar en cada laboratorio un comentario de acuerdo a cada acción realizada, considerando, ¿qué sucede?, ¿por qué transmite?, ¿cómo se transmite?*

1. Implementar un dominio de colisión con 10 equipos:



Ejecute	Resultados
a. Activar la opción de Observar los niveles de capas.	-----
b. Transmisión de un equipo a otro.	Se transmite sin problemas, llegando al destino.
c. Transmisión de dos o más equipos.	Se generan colisiones dependiendo del modo (half duplex o full duplex).
d. Generar una colisión.	Al haber una colisión los equipos vuelven a reenviar después de un tiempo aleatorio.
e. Generar dos colisiones.	Al haber dos o más colisiones los equipos vuelven a reenviar data. Se aprecia una latencia mayor.
f. Guardar la configuración realizada.	-----

2. Implementar tres dominios de colisión con dispositivos de capa 2:



Ejecute	Resultados
a. Seleccione el Modo simulación.	-----
• Transmisión de un equipo dentro de un dominio de colisión.	En un puerto del switch se aprecia que solamente transmite dentro de ese puerto.
• Transmisión de dos o más equipos hacia diferentes dominios de colisión.	Se aprecia que no hay colisiones, salvo que dos equipos de un mismo dominio envíen datos a la vez.
• Generar una colisión en cada dominio de forma individual.	Al haber una colisión los equipos vuelven a reenviar después de un tiempo aleatorio pero no se afecta a otro dominio de colisión.
• Generar una colisión en cada dominio de forma paralela.	Al haber una colisión los equipos vuelven a reenviar después de un tiempo aleatorio pero no se afecta a otro dominio de colisión.

FASE II: Configuración en su equipo:

Para su implementación deberá tener una red de dos a cuatro equipos.

a. Desinstalar la tarjeta de red (revisar anexos).

b. Instalar la tarjeta de red (revisar anexos).

c. Establecer una red de dos a cuatro equipos con una dirección privada en clase C.

d. Modifique su configuración en las propiedades de la NIC:

i. Acceda a las opciones avanzadas.

ii. Modifique el valor de su configuración.

iii. Compruebe qué sucede e indique si en alguna de las configuraciones no existe conectividad o acceso con el destino:

Modo de trabajo		Resultado
Automático		Establece una negociación con el punto de switch y no debe existir problemas de transmisión.
Full duplex 100mbps	Modo completo 100	Puede influir en cierto modo la marca de la tarjeta, aunque deberá deshabilitarse de acuerdo al modo de operación.
Half duplex 100mbps	Modo medio 100	
Full duplex 10mbps	Modo completo 10	
Half duplex 10mbps	Modo medio 10	

e. Responda las siguientes preguntas:

i. ¿Puede su equipo comunicarse con otro equipo que tenga una dirección IP diferente? ¿Por qué?

Rpta. Sí, debido a que las redes están implementadas para trabajar de esa manera, pero debe basarse en ciertas reglas del direccionamiento IP, además que el switch al trabajar en capa 2 verifica sólo las direcciones MAC.

ii. Si se tiene un switch como concentrador, ¿se podrán producir colisiones? ¿Por qué?

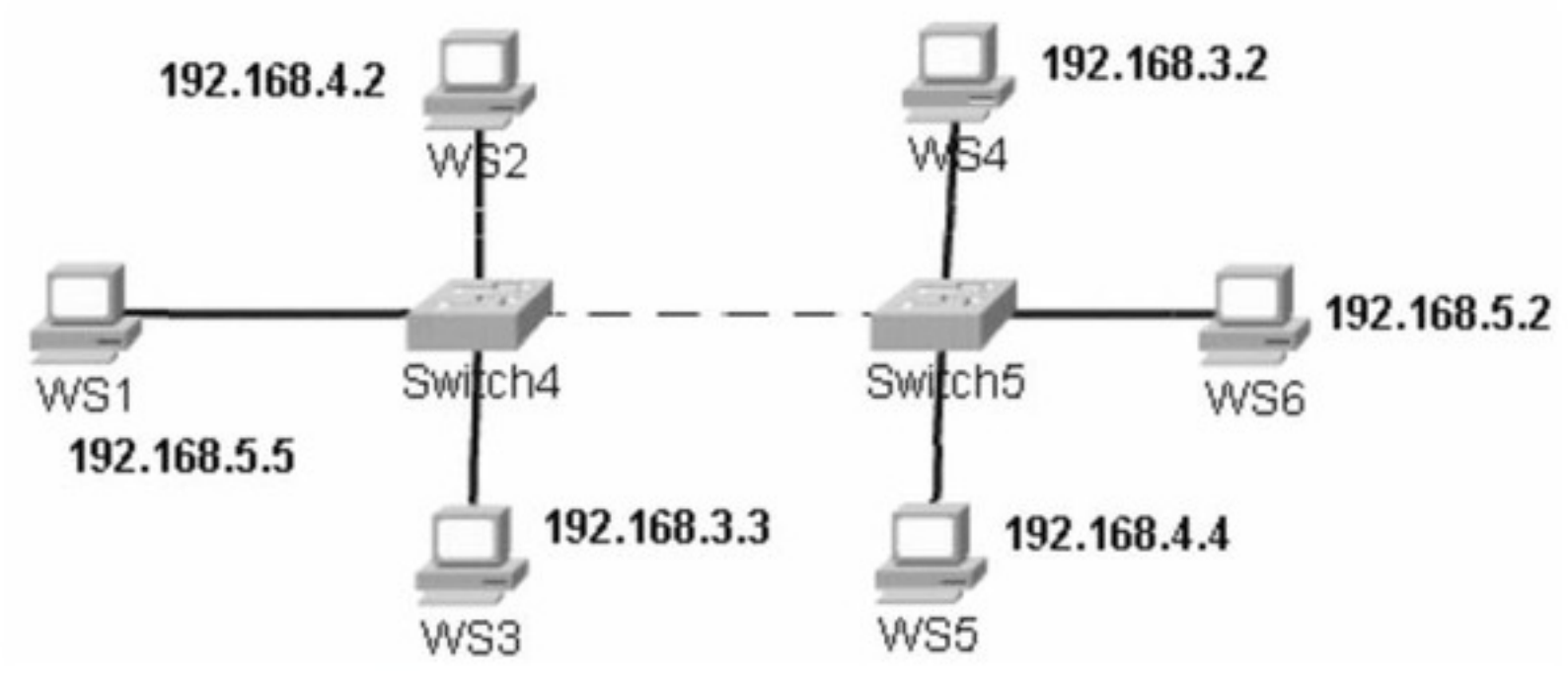
Rpta. No, porque a cada puerto del switch se asigna un microsegmento, estableciendo un dominio de colisión. Asimismo, al transmitir en full duplex, evita las colisiones.

iii. ¿Cuántos dominios de colisión se podrán establecer con un **HUB** como concentrador y luego con un **SWICHT**? ¿Por qué?

Rpta. Con un hub se puede establecer sólo un dominio de colisión y con un switch se puede tener un dominio de colisión en cada puerto conectado.

FASE III: Empleando el simulador "Packet tracer"

1. Implementar el siguiente esquema de red:



a. ¿Cuántos dominios de colisión existen en el gráfico? ¿Por qué?

Rpta. Hay siete dominios de colisión, ya que cada puerto en uso permite un dominio de colisión.

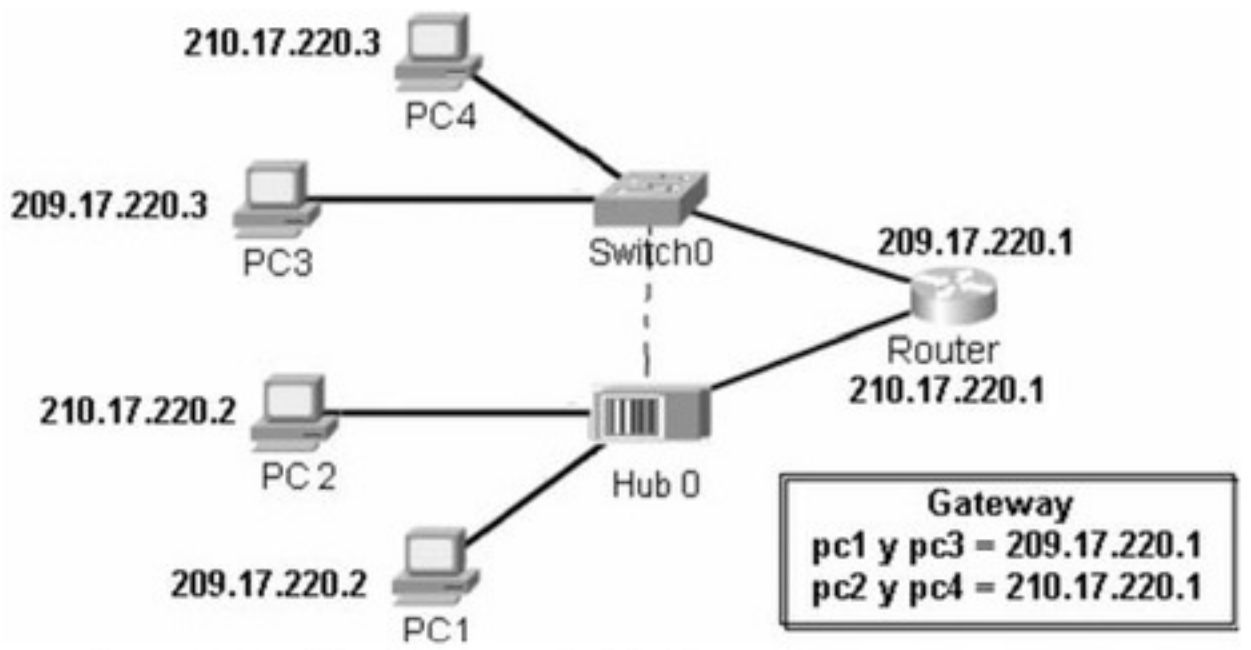
2. Realizar las siguientes pruebas:

1. Configure todos los puertos del switch en modo half duplex a 10 Mbps.	
EJECUTE	**RESULTADOS**
• Transmisión de un equipo a otro.	Se hace de manera rápida, sin colisiones
• Transmisión de tres equipos hacia sus pares en la red.	Se presentan muchas colisiones.
• ¿Por qué ocurren dichas situaciones?	Se debe al modo de trabajo half duplex, además de que los switches se encuentran aprendiendo las MAC de cada Host.

2. Configure todos los puertos del switch en modo half duplex a 100 Mbps.	
EJECUTE	**RESULTADOS**
• Repita los mismos pasos anteriores.	Sigue habiendo problemas de colisión.
• ¿Se genera la misma situación anterior? ¿Por qué?	No se producen colisiones, por lo que el modo automático está trabajando a full duplex según las capacidades de los equipos.

3. Configure todos los puertos del switch en modo automático.	
EJECUTE	**RESULTADOS**
▪ Repita los mismos pasos anteriores.	Se trata de una red actual donde no habrá colisiones.
▪ ¿Se genera la misma situación anterior? ¿Por qué?	No se producen colisiones, por lo que el modo automático está trabajando a full duplex según las capacidades de los equipos.

3. Ejecute la siguiente configuración:



a. Realice las pruebas necesarias de conectividad.

b. Pruebe transmitir datos entre los Host, en los diferentes modos de transmisión.

c. Reemplace el hub por un switch y haga las pruebas nuevamente.

d. ¿Qué ventajas ofrece dicha conexión?

Rpta. Al dividir la red en más dominios de colisión, se puede dirigir el tráfico de datos a un solo equipo destino. A diferencia del hub, que transmite los datos por todos sus puertos, el switch realiza una verificación de la trama, obteniendo la dirección MAC destino, compara con su tabla y transmite sólo mediante el puerto al equipo destino.

OBSERVACIONES

LABORATORIO 2 - CARGA DEL SWITCH

DESCRIPCIÓN

Durante el proceso de configuración, un switch debe tener una correcta carga del sistema operativo ya que sin ello no funcionaría; además, debe estar limpio de cualquier configuración anterior porque el hecho de trabajar sin eliminarla complicaría el trabajo a realizar, produciendo diagnósticos errados, entre otras cosas.

OBJETIVOS

1. Identificar la secuencia de carga de un switch.
2. Eliminar adecuadamente la configuración de un switch.

PLANTEAMIENTO

1. ELIMINANDO LA CONFIGURACIÓN DE UN SWITCH:

Considerando que se tiene acceso al equipo mediante el puerto consola, a la vez que no hay problemas con las contraseñas de acceso, se deberá eliminar la configuración siempre que se encuentre una configuración anterior.

Elimine la configuración de la NVRAM mediante el comando **erase startup-config** o **erase nvram**, pero si se ha creado vlan o algo parecido, deberá eliminar el archivo Vlan.dat de la memoria Flash (**delete vlan.dat**). Luego de ello reinicie el switch para completar el proceso.

```
Switch con0 is now available

Press RETURN to get started.

Switch>
Switch>ena
                                    //-en la línea siguiente se elimina la configuración
Switch#erase nvram
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
Erase of nvram: complete
01:07:51: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram

                                    //-en la línea siguiente se elimina el archivo Vlan.dat
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]y
%Error deleting flash:vlan.dat (No such file or directory)

                                    //-en la línea siguiente se reinicia el equipo Switch#reload
Proceed with reload? [confirm]y
01:08:01: %SYS-5-RELOAD: Reload requested
```

***Nota**: Tener cuidado de eliminar el IOS de la memoria Flash durante el proceso anterior.*

2. CARGA DEL SWITCH

Es un proceso que sigue una secuencia lógica de diagnóstico y carga de archivos mediante el software del cargador de arranque ubicado en la NVRAM:

1. Inicialización del CPU, registros y otros
2. POST → Diagnóstico de hardware
3. Flash → Acceso a la carpeta con el nombre del IOS o subdirectorios
4. Flash → Carga de la imagen del IOS con extensión .bin
5. Flash → El IOS se ejecuta utilizando el archivo config.text

```
//---------------------------------- PASOS 1 y 2

C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)

Compiled Mon 22-Jul-02 17:18 by antonino

WS-C2950-24 starting...
Base ethernet MAC Address: 00:0d:29:d8:fc:00
Xmodem file system is available.
Initializing Flash...

flashfs[0]: 318 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 5506560
flashfs[0]: Bytes available: 2234880
flashfs[0]: flashfs fsck took 7 seconds.

...done initializing flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

//---------------------------------- PASOS 3 y 4

Loading "flash:/c2950-i6k2l2q4-tar.121-22.EA11/c2950-i6k2l2q4-mz.121-22.EA11.bin"...############
################################################################################
################################################################################
############################################################

File "flash:/c2950-i6k2l2q4-tar.121-22.EA11/c2950-i6k2l2q4-mz.121-22.EA11.bin" uncompressed and
installed, entry point: 0x80010000

//-en la línea anterior se muestra el acceso a la carpeta
con el nombre del IOS

executing...

        Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and
subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec.
252.227-7013.
```

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA11, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Tue 08-Jan-08 11:12 by amvarma
Image text-base: 0x80010000, data-base: 0x80680000

Initializing flashfs...
flashfs[1]: 318 files, 6 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 7741440
flashfs[1]: Bytes used: 5506560
flashfs[1]: Bytes available: 2234880
flashfs[1]: flashfs fsck took 7 seconds.
flashfs[1]: Initialization complete.
Done initializing flashfs.
POST: System Board Test : Passed
POST: Ethernet Controller Test : Passed
ASIC Initialization Passed

POST: FRONT-END LOOPBACK TEST: Passed
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C2950-24 (RC32300) processor (revision J0) with 19912K bytes of memory.
Processor board ID FHK0726W1PF
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

//-en la línea siguiente se muestra un resumen del hardware en el switch.

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:0D:29:D8:FC:00
Motherboard assembly number: 73-5781-11
Power supply part number: 34-0965-01
Motherboard serial number: FOC07251QSE
Power supply serial number: DAB07247KJH
Model revision number: J0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0726W1PF

//---------- PASO 5

En este caso el archivo config.text está vacío, por lo que la línea siguiente muestra el cuadro de diálogo para la asistencia en la configuración

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
00:00:13: %ENVIRONMENT-2-FAN_FAULT: System Fault: FAN FAULT is detected.
00:00:16: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:19: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA11, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Tue 08-Jan-08 11:12 by amvarma
00:00:19: %SNMP-5-COLDSTART: SNMP agent on host Switch is undergoing a cold start
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Todo cuadro de diálogo se cancela colocando "no", y en caso de colocar "yes", se cancela con las teclas Ctrl + C.

```
Press RETURN to get started!

Switch>
00:01:47: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
```

LABORATORIO 3 - DETERMINANDO CARACTERÍSTICAS EN LOS SWITCHES

DESCRIPCIÓN

La implementación de una red LAN exige manejar apropiadamente la configuración de switch, considerando las opciones básicas y avanzadas. El presente ejercicio permite revisar criterios de implementación básica, desde la configuración de nombre, contraseñas y direccionamiento IP.

OBJETIVOS

- Implementar las opciones básicas de configuración en un switch.
- Realizar el diagnóstico de equipos vecinos característicos.

PLANTEAMIENTO

FASE I:

1. Verifique el funcionamiento del switch.
2. Elimine toda configuración anterior.
3. Realizar la configuración básica del switch, incluyendo el acceso vía Telnet.

FASE II:

1. Establecer la conexión de switch en una topología en malla (3 a 4).
2. Conectar adicionalmente un host para cada switch.
3. Configure una dirección IP para cada switch y Host, de tal manera que estén en una sola red.
4. Complete el recuadro con las características de su equipo:

	Características
Sistema operativo / versión	WINDOWS XP
Nombre de equipo	PC1
Dirección(es) MAC	0002-1671-BE5D
Nº IP	172.17.0.1
Máscara de subred	255.255.255.0
Puerta de enlace	172.17.0.254

FASE III:

1. Dirección asignada a su Host: 192.168.33.11.
2. Realizar un ping a varios Host de su red establecida, incluidos los switches.
3. Ejecute el comando **ARP –a** y complete la tabla.

```
PC>ARP -A
  Internet Address      Physical Address      Type
  192.168.33.2          000a.4191.1118        dynamic
  192.168.33.3          00e0.8f34.639e        dynamic
  192.168.33.4          0090.0cba.d785        dynamic
  192.168.33.5          0002.176a.e762        dynamic
  192.168.33.12         0005.5eee.7dd2        dynamic
  192.168.33.13         0030.f2c2.39cd        dynamic
  192.168.33.14         000a.41a6.0ad0        dynamic
```

	MAC	IP	Nombre del Host
1.	0005-5EEE-7DD2	192.168.33.12	PC2
2.	0030-F2C2-39CD	192.168.33.13	PC3
3.	000A-41A6-0AD0	192.168.33.14	PC4

FASE IV:

- Acceda a cada switch y determine sus características.
- Para ello puede hacerse uso de los comandos:

Comandos	Descripción
• Show cdp neighbors	Resumen de vecinos Cisco conectados.
• Show cdp neighbors retail	Detalle de vecinos Cisco conectados.
• Show running-config	Configuración actual de switch.
• Show version	Datos del hardware, IOS y otras características.
• Telnet x.x.x.x	Acceso remoto a un equipo.

Como se puede comprobar, a continuación pueden obtenerse los datos de un equipo vecino con los comandos listados sin necesidad de acceder al otro equipo, salvo que fuesen datos más específicos, como la configuración activa de cada switch o sus resultados de VTP, VLAN, STP, etc.

```
Sw2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme   Capability   Platform   Port ID
SW1             Fas 0/3        160         S          2950     Fas 0/2
SW3             Fas 0/2        148         S          2950     Fas 0/1
SW4             Fas 0/1        121         S          2950     Fas 0/1
```

```
Sw2#sh cdp neighbors detail
Device ID: SW1
Entry address(es):
  IP address : 192.168.33.2
Platform: Cisco 2950, Capabilities: Switch
Interface: FastEthernet0/3, Port ID (outgoing port): FastEthernet0/2
Holdtime: 155
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full
---------------------------

< resultado omitido >
```

```
Sw2#sh version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000
ROM: Bootstrap program is is C2950 boot loader
Switch uptime is 9 hours, 11 minutes, 34 seconds
System returned to ROM by power-on
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)
32K bytes of flash-simulated non-volatile configuration memory.
Base Ethernet MAC Address: 00E0.8F34.639E
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF
```

a. Tabla de resumen:

La siguiente tabla se completó mediante el uso de los comandos anteriores: primeramente, lo del switch local, con **show running-config**, **show version** y **show flash**, seguidos del **show cdp neighbors detail** y luego el acceso vía **Telnet**.

Características	SW-1	SW-2	SW-3	SW-4
Plataforma	WS-C2950-24	WS-C2950-24	WS-C2950-24	WS-C2950-24
IOS	c2950-i6q4l2-mz.121-22.EA4.bin	c2950-i6q4l2-mz.121-22.EA4.bin	c2950-i6q4l2-mz.121-22.EA4.bin	c2950-i6q4l2-mz.121-22.EA4.bin
Versión	12.1	12.1	12.1	12.1
Nº IP	192.168.33.2	192.168.33.3	192.168.33.4	192.168.33.5
Nº de puertos	24	24	24	24
Velocidad de puertos	10/100	10/100	10/100	10/100
Contraseña de consola	Cisco	Cisco	Cisco	Cisco
Contraseña VTY	class	class	class	class
MAC BASE	000A.4191.1118	00E0.8F34.639E	0090.0CBA.D785	0002.176A.E762

b. Capturar la información de las direcciones estáticas y dinámicas de cada switch.

- La lista de direcciones MAC que aparece a continuación es obtenida mediante las tramas recibidas en los puertos que se indican, permanece un tiempo y luego se elimina automáticamente.
- En el tipo de dirección MAC puede aparecer **dynamic**, ya que se considera que es una dirección que puede cambiar, pero también puede aparecer **static**, que generalmente son las MAC asociadas al mismo switch.

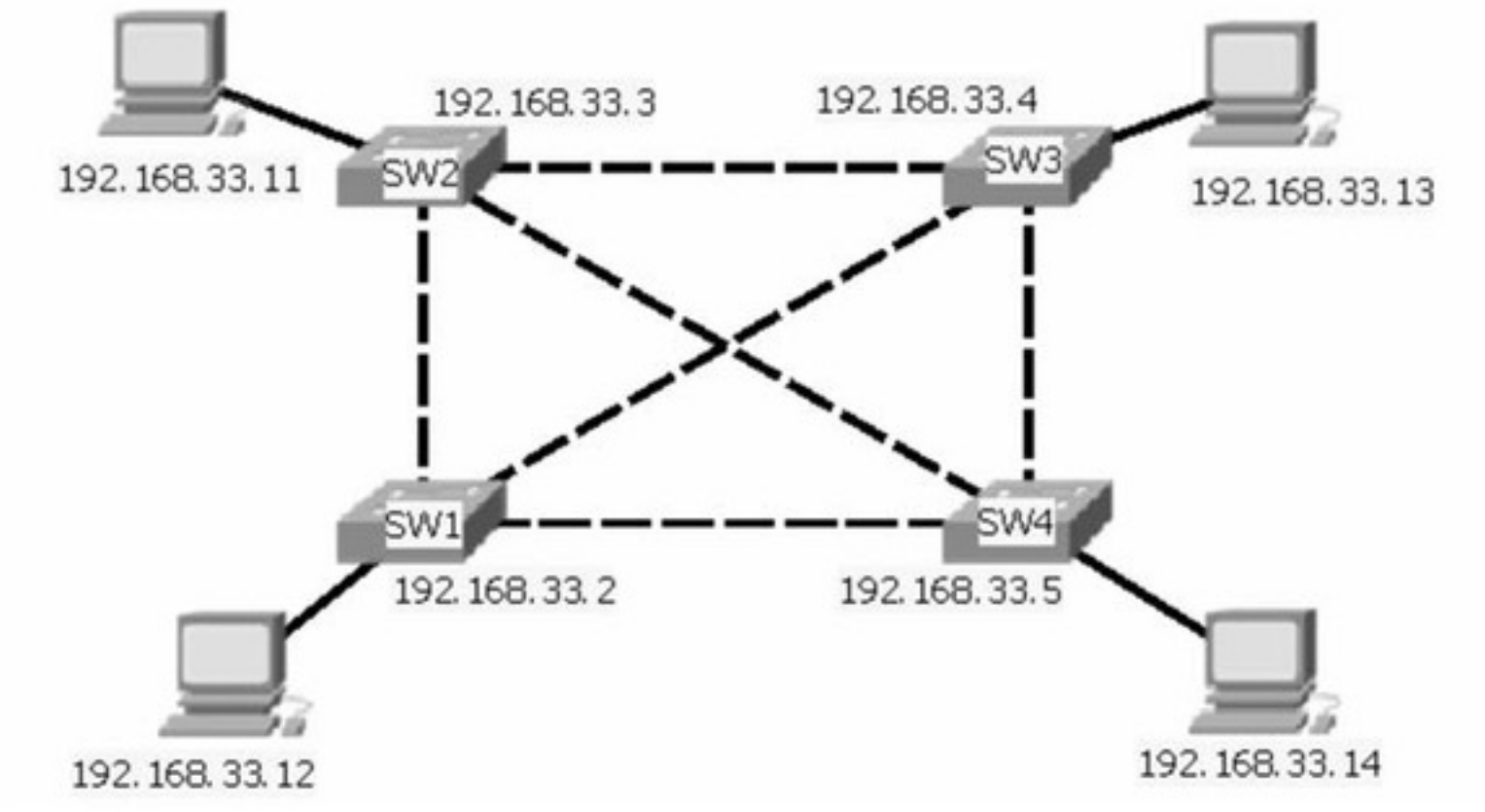
```
SW1#sh mac-address-table
        Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0002.1671.be5d    DYNAMIC     Fa0/1
   1    0002.176a.e762    DYNAMIC     Fa0/1
   1    0005.5eee.7dd2    DYNAMIC     Fa0/4
   1    000a.41a6.0ad0    DYNAMIC     Fa0/1
   1    0030.f2c2.39cd    DYNAMIC     Fa0/1
   1    0050.0f75.c902    DYNAMIC     Fa0/1
   1    0090.0cba.d785    DYNAMIC     Fa0/1
   1    00e0.8f34.639e    DYNAMIC     Fa0/1
```

```
SW2# sh mac-address-table
        Mac Address Table
------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0002.1671.be5d    DYNAMIC     Fa0/4
   1    0002.176a.e762    DYNAMIC     Fa0/1
   1    0005.5eee.7dd2    DYNAMIC     Fa0/1
   1    000a.4191.1118    DYNAMIC     Fa0/1
   1    000a.41a6.0ad0    DYNAMIC     Fa0/1
   1    0030.f2c2.39cd    DYNAMIC     Fa0/1
   1    0050.0f75.c901    DYNAMIC     Fa0/1
   1    0090.0cba.d785    DYNAMIC     Fa0/1
```

```
SW3#sh mac-address-table
        Mac Address Table
------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0002.1671.be5d    DYNAMIC     Fa0/2
   1    0002.176a.e762    DYNAMIC     Fa0/2
   1    0005.5eee.7dd2    DYNAMIC     Fa0/2
   1    000a.4191.1118    DYNAMIC     Fa0/2
   1    000a.41a6.0ad0    DYNAMIC     Fa0/2
   1    0030.f2c2.39cd    DYNAMIC     Fa0/4
   1    0050.0f75.c903    DYNAMIC     Fa0/2
   1    00e0.8f34.639e    DYNAMIC     Fa0/2
```

```
SW4#sh mac-address-table
        Mac Address Table
------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0002.1671.be5d    DYNAMIC     Fa0/1
   1    0002.4a08.b701    DYNAMIC     Fa0/1
   1    0005.5eee.7dd2    DYNAMIC     Fa0/2
   1    000a.4191.1118    DYNAMIC     Fa0/2
   1    000a.41a6.0ad0    DYNAMIC     Fa0/4
   1    0030.f2c2.39cd    DYNAMIC     Fa0/3
   1    0090.0cba.d785    DYNAMIC     Fa0/3
   1    00d0.979e.e902    DYNAMIC     Fa0/3
   1    00e0.8f1a.d001    DYNAMIC     Fa0/2
   1    00e0.8f34.639e    DYNAMIC     Fa0/1
```

c. Diseño lógico de la red establecida.



OBSERVACIONES

LABORATORIO N° 4 - IMPLEMENTACION DE VLAN EN UN DOMINIO VTP

DESCRIPCIÓN

La implementación de Lan virtuales facilita la administración de la red y el control de broadcast, a su vez complementadas mediante un dominio VTP que otorga mayor seguridad y escalabilidad a la red.

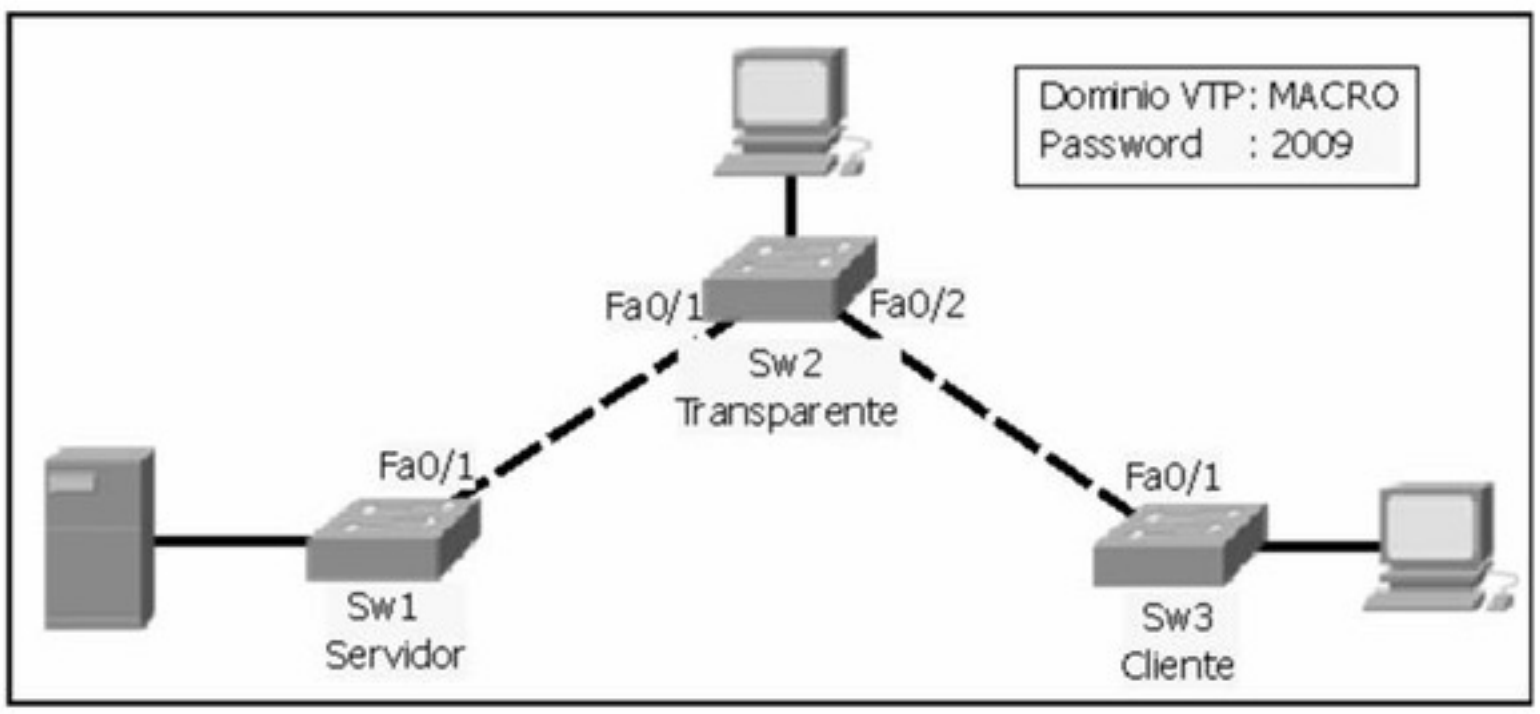
El dominio se establece mediante un esquema cliente-servidor, intercambiando mensajes de actualización donde se propaga cualquier información de Vlan, sólo entre equipos que manejen un nombre y contraseña en común.

OBJETIVOS

- Establecer una red que permita identificar los elementos necesarios de un dominio VTP.
- Configurar las opciones mínimas de seguridad en los switches.

PLANTEAMIENTO

1. Implementar una red con las siguientes características:



2. Considerar la siguiente cantidad de Host por Vlan:

VLAN	10	20	30	40	50
N° HOST	20	15	15	50	40

3. Características VTP en cada switch:

Nombre del switch	Modo VTP	Host para Vlan
SW1- Server	Server	10, 20, 30
SW2- Transparent	Transparent	10, 30, 50
SW3- Client	Client	40, 50

4. Adicionalmente, crear un VLAN 77 que trabaje como Vlan administrativa, donde cada switch deberá tener asignado un puerto para la administración.
5. Habilitar la seguridad de puerto en cada switch, considerando el número máximo de Host.
6. Almacenar en un servidor TFTP el IOS y el archivo de configuración.
7. Definir en los enlaces troncales el número de Vlan que pueda transmitir, así como la VLAN nativa.

SOLUCIÓN

FASE 1: CONFIGURACIÓN BÁSICA

1. La resolución del direccionamiento IP se realizó mediante el VLSM, empleando la dirección privada 192.168.210.0, y se distribuyó de la siguiente forma.

ÁREA	Vlan	N° DE HOST	ID DE RED	MÁSCARA DE SUBRED
A.C.	40	50	192.168.210.0/26	255.255.255.192
Ventas	50	40	192.168.210.64/26	255.255.255.192
Contabilidad	10	20	192.168.210.128/27	255.255.255.224
M.D.	20	15	192.168.210.160/27	255.255.255.224
RR.HH.	30	15	192.168.210.192/27	255.255.255.224
H. D.	77	6	192.168.210.248/29	255.255.255.240

2. Realizar la eliminación de cualquier configuración anterior.
3. Configurar las opciones básicas en cada switch.
4. Por seguridad, los puertos del switch deben ser de acceso y estar deshabilitados, e ir habilitándose conforme se utilicen, comenzando por los puertos troncales; recuerde que los puertos están activos por defecto y en modo auto, lo que podría permitirles automáticamente convertirse en troncal.
5. Se deberá implementar la conexión física de los equipos, según el esquema.

```
TRANSPARENT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRANSPARENT(config)#interface range f0/1 - 24
TRANSPARENT(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
……..< resultado omitido >
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
TRANSPARENT(config-if-range)#exit
TRANSPARENT#
```

- Para el caso anterior, los puertos 1 y 2 del switch ya habían estado activados por conexión hacia los switch 1 y 2; nótese que al desactivarse tienen mensajes diferentes del resto de puertos.

FASE 2: CONFIGURACIÓN VTP

1. Toda configuración de VTP debe definirse, inicialmente, con el modo de operación, el nombre del dominio, la contraseña y su versión VTP.
   - Para este caso se realiza en el switch 2, pero continúe la configuración en los siguientes switches.

```
TRANSPARENT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRANSPARENT(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
TRANSPARENT(config)#vtp domain MACRO
Changing VTP domain name from NULL to MACRO
TRANSPARENT(config)#vtp password 2009
Setting device VLAN database password to 2009
TRANSPARENT(config)#vtp version 2
TRANSPARENT(config)#
```

FASE 3: CONFIGURACIÓN DE VLAN Y PUERTOS TRONCALES

La siguiente configuración se muestra ejecutándose en el switch 1 y deberá ser replicada en el switch 3.

- **Definiendo las Vlan a emplear.**

  Se configuran las Vlan en los switches Server y Transparent, considerando que el modo cliente sólo recibe las Vlan creadas en el Server.

```
TRANSPARENT(config)#vlan 10
TRANSPARENT(config-vlan)#name vlan10_192_168_210_128_26
TRANSPARENT(config-vlan)#vlan 20
TRANSPARENT(config-vlan)#name vlan20_192_168_210_160_27
TRANSPARENT(config-vlan)#vlan 30
TRANSPARENT(config-vlan)#name vlan30_192_168_210_192_27
TRANSPARENT(config-vlan)#vlan 40
TRANSPARENT(config-vlan)#name vlan40_192_168_210_0_26
TRANSPARENT(config-vlan)#vlan 50
TRANSPARENT(config-vlan)#name vlan50_192_168_210_64_26
TRANSPARENT(config-vlan)#vlan 77
TRANSPARENT(config-vlan)#name vlan77_192_168_210_248_26
TRANSPARENT(config-vlan)#end
TRANSPARENT#
```

- **Modificando la Vlan administrativa**

  Establecer la Vlan 77 como administrativa y nativa, de tal manera que la Vlan por defecto (Vlan 1) sea modificada por seguridad; asimismo, las tramas que esta Vlan envíe por los puertos troncales no serán etiquetadas.

```
TRANSPARENT#
TRANSPARENT#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TRANSPARENT(config)#interface vlan 77
TRANSPARENT(config-if)#ip address 192.168.210.250 255.255.255.248
TRANSPARENT(config-if)#no shutdown
TRANSPARENT(config-if)#
```

- **Definiendo puertos troncales**

  Definir en los enlaces troncales el número de cada Vlan que podrá transmitir tramas; recuerde que los puertos troncales deberán contemplar el paso de todas las Vlan, así el switch no tenga puertos asignados. También se debe indicar la nueva Vlan nativa.

```
TRANSPARENT(config)#interface range f0/1 - 2
TRANSPARENT(config-if-range)#switchport mode trunk
TRANSPARENT(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
TRANSPARENT(config-if-range)#switchport native vlan 77
TRANSPARENT(config-if-range)#switchport trunk allowed
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (77),
with Switch FastEthernet0/1 (1).vl
TRANSPARENT(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,77
TRANSPARENT(config-if-range)#^Z
%SYS-5-CONFIG_I: Configured from console by console
TRANSPARENT#wr
Building configuration...
[OK]
TRANSPARENT#
```

  El mensaje que aparece al configurar el switch corresponde a la falta de configuración en los otros switches respecto a la Vlan nativa que ahora será la Vlan 77.

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (77), with
Switch FastEthernet0/1 (1).vl
```

- **Asignando puertos a cada Vlan**

1. Seleccione los puertos agrupándolos con el comando **range** y asígnelos a las Vlan definidas. Asimismo, establezca la seguridad de puerto para un máximo de direcciones de acuerdo a los Host por Vlan.
2. Complemente con la Vlan administrativa y asígnele un puerto.

```
TRANSPARENT(config)#
TRANSPARENT(config)#interface range f0/3 - 9
TRANSPARENT(config-if-range)#switchport access vlan 10
TRANSPARENT(config-if-range)#switchport mode access
TRANSPARENT(config-if-range)#switchport port-security maximum 30
TRANSPARENT(config-if-range)#switchport port-security mac-address sticky
TRANSPARENT(config-if-range)#
```

3. Realizar las pruebas de conectividad entre los diferentes equipos, switches y PC.

   Recordar que no puede existir conectividad entre equipos de una Vlan con otra Vlan, por tratarse de subredes diferentes y por la falta de enrutamiento.
4. Almacene en el servidor TFTP el IOS, así como la configuración realizada.

CONFIGURACION FINAL

A continuación, la configuración final de cada switch.

1. CONFIGURACIÓN FINAL DEL SWITCH SERVER

```
SERVER#show running-config
Building configuration...
Current configuration : 4184 bytes
!
version 12.1
no service password-encryption
!
hostname SERVER
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 77
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 30
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 30
 switchport port-security mac-address sticky
!
……..<  resultado omitido  >
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan77
 ip address 192.168.210.249 255.255.255.248
!
no cdp run
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

```
SERVER#show vlan
VLAN Name                              Status    Ports
---- --------------------------------  --------- -------------------------------
1    default                           active
10   10_192_168_210_128_27             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8
20   20_192_168_210_160_27             active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   30_192_168_210_192_27             active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23
40   40_192_168_210_0_26               active
50   50_192_168_210_64_26              active
77   77_192_168_210_248_29             active    Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

.....< resultado omitido>
```

```
SERVER#show vtp status
VTP Version                     : 2
Configuration Revision          : 12
Maximum VLANs supported locally : 255
Number of existing VLANs        : 11
VTP Operating Mode              : Server
VTP Domain Name                 : lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     |          : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB3 0xA8 0x6E 0x0F 0x3C 0x71 0xA6 0xC6
Configuration last modified by 0.0.0.0 at 3-1-93 03:46:26
Local updater ID is 192.168.210.249 on interface Vl77 (lowest numbered VLAN interface found)
```

2. CONFIGURACIÓN FINAL DEL SWITCH TRANSPARENTE

```
TRANSPARENT#show running-config
Building configuration...
Current configuration : 4393 bytes
version 12.1
no service password-encryption
!
hostname TRANSPARENT
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip domain-lookup
!
vtp domain MACRO
vtp mode transparent
vtp password 2009
!
```

```
vlan 10
 name 10_192_168_210_128_27
!
vlan 20
 name 20_192_168_210_160_27
!
vlan 30
 name 30_192_168_210_192_27
!
vlan 40
 name 40_192_168_210_0_26
!
vlan 50
 name 50_192_168_210_64_26
!
vlan 77
 name 77_192_168_210_248_29
!
interface FastEthernet0/1
 switchport trunk native vlan 77
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 77
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 30
 switchport port-security mac-address sticky
!
.....< resultado omitido >
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan77
 ip address 192.168.210.250 255.255.255.248
!
no cdp run
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

```
TRANSPARENT#show vlan
VLAN Name                              Status    Ports
---- --------------------------------  --------- -------------------------------
1    default                           active
10   10_192_168_210_128_27             active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9
20   20_192_168_210_160_27             active
30   30_192_168_210_192_27             active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16
40   40_192_168_210_0_26               active
50   50_192_168_210_64_26              active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23
77   77_192_168_210_248_29             active    Fa0/24

.....< resultado omitido >
```

```
TRANSPARENT#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 11
VTP Operating Mode              : Transparent
VTP Domain Name                 : lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x81 0xFF 0x03 0x99 0x54 0xED 0xE6 0x77
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

3. CONFIGURACIÓN FINAL DEL SWITCH CLIENTE

```
CLIENT#show running-config
Building configuration...
Current configuration : 4184 bytes
!
version 12.1
no service password-encryption
!
hostname CLIENT
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 77
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 40
 switchport mode access
 switchport port-security maximum 50
 switchport port-security mac-address sticky
```

```
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport mode access
 switchport port-security maximum 50
 switchport port-security mac-address sticky
!
.....< resultado omitido >
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan77
 ip address 192.168.210.251 255.255.255.248
!
no cdp run
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

```
CLIENT#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   10_192_168_210_128_27             active
20   20_192_168_210_160_27             active
30   30_192_168_210_192_27             active
40   40_192_168_210_0_26               active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11
50   50_192_168_210_64_26              active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
77   77_192_168_210_248_29             active    Fa0/24

.....< resultado omitido >
```

```
CLIENT#show vtp status
VTP Version                     : 2
Configuration Revision          : 12
Maximum VLANs supported locally : 255
Number of existing VLANs        : 11
VTP Operating Mode              : Client
VTP Domain Name                 : lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB3 0xA8 0x6E 0x0F 0x3C 0x71 0xA6 0xC6
Configuration last modified by 0.0.0.0 at 3-1-93 03:46:26
```

TAREA: Evitar que los broadcasts de una Lan lleguen a un switch donde no existan puertos habilitados.

***Nota**: La configuración completa del laboratorio se encuentra en el CD-ROM que acompaña este material.*

OBSERVACIONES

_____

_____

_____

_____

LABORATORIO N° 5 - IMPLEMENTACIÓN DE VLAN, CON UN DOMINIO VTP Y STP

DESCRIPCIÓN

El protocolo de spanning tree facilita la implementación de una red al desactivar enlaces redundantes que establezcan bucles de capa 2, lo cual evita la propagación de las tormentas broadcast y las tablas de direcciones MAC inconsistentes.

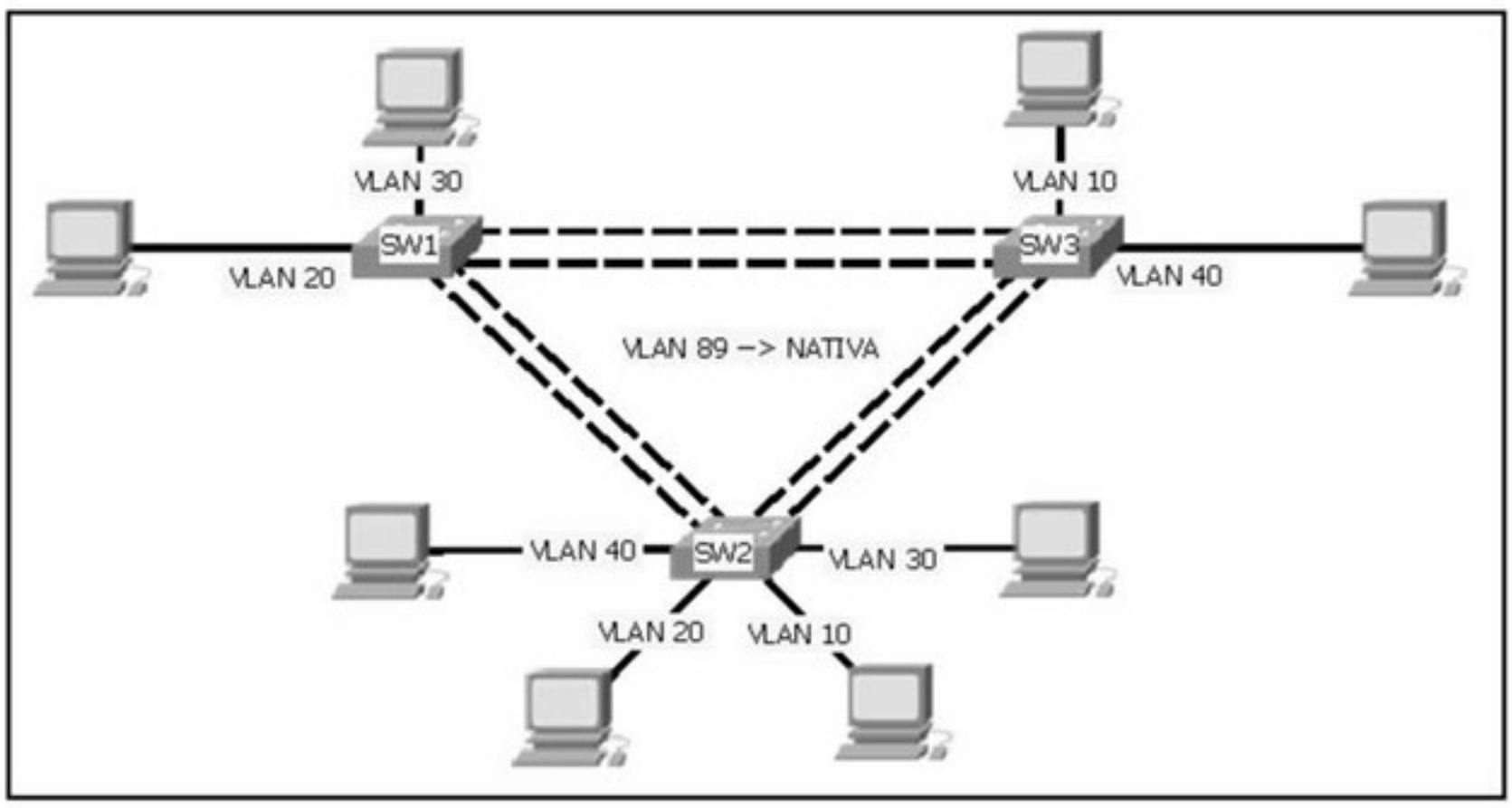
Por defecto, los switches manejan este protocolo, pero muchas veces es necesario modificar dichas opciones y establecer con mayor criterio una configuración más óptima para la red; por eso, el presente laboratorio integra la configuración de un dominio VTP con el protocolo spanning tree, permitiendo modificar algunas características por defecto.

OBJETIVOS

- Configurar los elementos para el funcionamiento de spanning tree en un dominio VTP.
- Establecer criterios para optimizar una red con spanning tree.

PLANTEAMIENTO

- Implementar el siguiente esquema de red.



- Considerar la siguiente cantidad de Host por Vlan.

vlan	10	20	30	40	89
host	11	22	33	44	8

- El dominio VTP deberá tener las siguientes características.

Dominio	cisco2
Password	class
SW1	Server
SW2	Cliente1
SW3	Transparente

- Spanning tree.

VLAN	Root Primary	Root Secondary
1	SW2	SW3
10	SW2	SW1
20	SW3	SW2
30	SW3	SW1
40	SW1	SW2

- Definir en los switches que las interfaces con mayor valor en número sean elegidas para VTP y no la de menor valor.

SOLUCIÓN

FASE 1: DIRECCIONAMIENTO IP

1. La tabla adjunta indica el direccionamiento IP definido para desarrollar el planteamiento.

Vlan	N° de Host	ID de red
10	11	192.168.100.160/28
20	22	192.168.100.128/27
30	33	192.168.100.64/26
40	44	192.168.100.0/26
89	8	192.168.100.240/28

FASE 2: CONFIGURACIÓN BÁSICA

1. Elimine cualquier configuración anterior encontrada en el switch.
2. Configure las opciones básicas en cada switch.
3. Al definir los puertos en modo acceso, por seguridad, se recomienda colocar los puertos en dicho modo y desactivarlos desde el primer momento. Recordar que los switches están activados por defecto y en modo auto.

```
SW1#conf term
SW1(config)#interface range fastethernet 0/21 - 24
SW1(config-if-range)#switchport mode access
00:01:51: %SYS-5-CONFIG_I: Configured from console by console
00:01:52: %SYS-5-CONFIG_I: Configured from console by console
SW1(config-if-range)#shutd
SW1(config-if-range)#end
```

4. Implementar la conexión física de acuerdo al diagrama.

FASE 3: CONFIGURACIÓN VTP

En esta fase se configura primeramente el protocolo VTP, lo cual permitirá propagar las Vlan al completar la configuración de Vlan y enlaces troncales. Según los requerimientos de implementación, configure el dominio VTP con el nombre **cisco2**, contraseña **class**, **versión 2**. Se presenta la configuración del switch 1 en modo Server; asimismo, configure los switches 2 y 3.

```
SW1#conf term
SW1(config)#vtp version 2
VTP mode already in V2.
SW1(config)#vtp mode server
Device mode already VTP SERVER.
SW1(config)#vtp domain cisco2
Changing VTP domain name from NULL to cisco2
SW1(config)#vtp password class
Setting device VLAN database password to class
SW1(config)#end
SW1#
```

FASE 4: CONFIGURACIÓN DE VLAN Y PUERTOS TRONCALES

La siguiente configuración se muestra ejecutándose en el switch 1 y deberá ser replicada en el switch 3.

- Definiendo las Vlan a emplear

  En este proceso de configuración se asignan los nombres a cada Vlan, considerando su identificador de red.

```
SW1(config)#vlan 10
SW1(config-vlan)#name vlan10_192_168_100_160_28
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name vlan20_192_168_100_128_27
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name vlan30_192_168_100_64_26
SW1(config-vlan)#vlan 40
SW1(config-vlan)#name vlan40_192_168_100_0_26
SW1(config-vlan)#vlan 89
SW1(config-vlan)#name vlan89_192_168_100_240_28
SW1(config-vlan)#end
SW1#
```

- Modificando la Vlan administrativa

  Deberá acceder a la interfaz de la Vlan 89, asignarle una dirección IP y activar la interfaz (con esto desactivamos la Vlan 1 como Vlan administrativa).

```
SW1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface vlan 89
SW1(config-if)#ip add 192.168.100.241 255.255.255.240
SW1(config-if)#no shutdown
SW1(config-if)#end
SW1#
```

- Definiendo puertos troncales

  Establecer los puertos definidos como troncales; asimismo, indicar que la Vlan nativa ha sido modificada por la Vlan 89.

```
SW1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int ran fa0/21 - 24
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# switchport trunk native vlan 89
SW1(config-if-range)#no shut
SW1(config-if-range)#end
SW1#
SW1#write
Building configuration...
```

- Asignando puertos a cada Vlan

  Seleccione los puertos agrupándolos con el comando **range** y asígnelos a las Vlan definidas. También asigne un puerto a la Vlan administrativa.

```
SW1#
SW1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface range fa0/1 - 5
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
SW1(config)# interface range fa0/6 - 10
SW1(config-if-range)# switchport access vlan 20
SW1(config-if-range)# no shutdown
SW1(config-if-range)# exit
SW1(config)# interface range fa0/11 - 14
SW1(config-if-range)# switchport access vlan 10
SW1(config-if-range)# no shutdown
SW1(config-if-range)# exit
SW1(config)# interface range fa0/15 - 19
SW1(config-if-range)# switchport access vlan 40
SW1(config-if-range)# no shutdown
SW1(config-if-range)# exit
SW1(config)# interface fa0/20
SW1(config-if)# switchport access vlan 89
SW1(config-if)# no shutdown
SW1(config-if)#end
SW1#write
Building configuration...
[OK]
```

- Verificando las Vlan creadas y puertos asignados:

```
SW1#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22
10   vlan10_192_168_100_160_28         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
20   vlan20_192_168_100_128_27         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
30   vlan30_192_168_100_64_26          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
40   vlan40_192_168_100_0_26           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19
89   vlan89_192_168_100_240_28         active    Fa0/20
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
SW1#write
00:37:53: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
```

FASE 5: CONFIGURACIÓN DE STP

- Al definir de esta forma el root primario, este switch se encarga de recibir los mensajes de actualización o emergencia de uno o más switches y replicar al resto de la red.
- Normalmente un solo equipo cumpliría la labor de root primario para todas la Vlan, pero esto se podría modificar para establecer un criterio de equilibrio de carga y así varios switches podrían participar en la elección.
- El establecerlo como primario da al switch la posibilidad de asegurarse que siempre será elegido para ese fin, en caso ingrese un switch nuevo. El switch secundario es el backup o reemplazo, si es que falla el primario.
- Para definir a un switch como root primary o root secondary se puede configurar de dos formas: una, con el comando **spanning.tree vlan xx Root primary** o **spanning.tree vlan xx root secondary**, y otra, variando directamente la prioridad, como se muestra, donde una prioridad más baja permitirá la elección como root primary o root secondary.

```
SW1#
SW1#conf term
SW1(config)#spanning-tree vlan 40 priority 4096
SW1(config)#spanning-tree vlan 10 priority 8192
SW1(config)#spanning-tree vlan 30 priority 8192
SW1(config)#end
SW1#write
Building configuration...
[OK]
```

- Al configurar la prioridad spanning tree para las interfaces troncales del switch, deberá considerar que por defecto el protocolo spanning tree desactiva la interfaz de mayor valor, ya que la prioridad por defecto es de 128 (al ser FastEthernet), sumando a ello el número de interfaz.

- Para modificar la prioridad del puerto deberá colocar un valor menor a 128 si es que se trata de interfaces FastEhernet, con valores que se incrementen de 16 en 16.

```
SW1#
SW1#conf term
SW1(config)#int fa0/24
SW1(config-if)#spanning-tree port-priority ?
  <0-240>  port priority in increments of 16
SW1(config-if)#spanning-tree port-priority 16
SW1(config-if)#int fa0/23
SW1(config-if)#spanning-tree port- priority 32
SW1(config-if)#int fa0/22
SW1(config-if)#spanning-tree port- priority 48
SW1(config-if)#int fa0/21
SW1(config-if)#spanning-tree port- priority 64
SW1(config-if)#end
SW1#
SW1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
SW1#write
Building configuration...
[OK]
```

***Nota**: Los mensajes que se visualizan son parte del proceso que ejecuta el protocolo STP para determinar qué enlaces tienen la menor prioridad y, de esa manera, establecer los puertos designados, raíz y no designado.*

- Verificando la configuración de spanning tree

  Debe tenerse en cuenta que todo switch en un primer momento se considerará como bridge root para todas las Vlan; conforme se intercambien los mensajes de BPDU, verificarán el valor de prioridad junto con la dirección MAC.

  Para el caso, el switch 1 se considera como **root primary** para todas las Vlan.

  Las Vlan tienen una prioridad de 32768 por defecto, pero a esto se sumará el valor de la Vlan. Compare para cada caso el valor prioridad que presenta el Bridge ID, en la mayoría de casos se tiene modificada la prioridad por defecto pero igual se le sumará el valor de la Vlan.

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000d.29d8.fc00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.29d8.fc00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg LRN 19          64.21   P2p
Fa0/22           Desg LIS 19         48.22   P2p
Fa0/23           Desg FWD 19          32.23   P2p
Fa0/24           Desg FWD 19          16.24   P2p
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    8202
             Address     000d.29d8.fc00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    8202   (priority 8192 sys-id-ext 10)
             Address     000d.29d8.fc00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg LRN 19        64.21   P2p
Fa0/22           Desg LRN 19        48.22   P2p
Fa0/23           Desg FWD 19         32.23   P2p
Fa0/24           Desg FWD 19         16.24   P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     000d.29d8.fc00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     000d.29d8.fc00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg LRN 19        64.21   P2p
Fa0/22           Desg LRN 19        48.22   P2p
Fa0/23           Desg FWD 19         32.23   P2p
Fa0/24           Desg FWD 19         16.24   P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    8222
             Address     000d.29d8.fc00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    8222   (priority 8192 sys-id-ext 30)
             Address     000d.29d8.fc00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg FWD 19        64.21   P2p
Fa0/22           Desg FWD 19        48.22   P2p
Fa0/23           Desg FWD 19        32.23   P2p
Fa0/24           Desg FWD 19        16.24   P2p

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    4136
             Address     000d.29d8.fc00
             This bridge is the root
```

```
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4136   (priority 4096 sys-id-ext 40)
        Address     000d.29d8.fc00
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 15
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19        64.21   P2p
Fa0/22          Desg FWD 19        48.22   P2p
Fa0/23          Desg FWD 19        32.23   P2p
Fa0/24          Desg FWD 19        16.24   P2p

VLAN0089
  Spanning tree enabled protocol ieee
  Root ID    Priority    32857
        Address     000d.29d8.fc00
        This bridge is the root
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
        Address     000d.29d8.fc00
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 15
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19        64.21   P2p
Fa0/22          Desg FWD 19        48.22   P2p
Fa0/23          Desg FWD 19        32.23   P2p
Fa0/24          Desg FWD 19        16.24   P2p
```

- Considere unos segundos para que la red entre en convergencia y verifique las configuraciones finales en cada uno de los switches.
- Realice las pruebas necesarias para comprobar su funcionamiento.

CONFIGURACIÓN FINAL

A continuación, la configuración final de cada switch.

1. CONFIGURACIÓN DEL SWITCH 1

```
SW1#show runn
Building configuration...
Current configuration : 2666 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$Z1Xy$Cxhk4LQE5px6Mrx5fgrQ50
ip subnet-zero
!
```

```
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1 priority 12288
spanning-tree vlan 10,30 priority 8192
spanning-tree vlan 40 priority 4096
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
……<resultado omitido>……
interface FastEthernet0/21
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 64
interface FastEthernet0/22
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 48
interface FastEthernet0/23
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 32
interface FastEthernet0/24
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 16
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan89
 ip address 192.168.100.241 255.255.255.240
 no ip route-cache
!
ip http server
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 9
Maximum VLANs supported locally : 128
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xAE 0x61 0x12 0x21 0x92 0x15 0x32 0x8F
Configuration last modified by 192.168.100.241 at 3-1-93 00:35:09
Local updater ID is 192.168.100.241 on interface Vl89 (lowest numbered VLAN interface found)
```

```
SW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/21    on        802.1q         trunking    89
Fa0/22    on        802.1q         trunking    89
Fa0/23    on        802.1q         trunking    89
Fa0/24    on        802.1q         trunking    89
Port      Vlans allowed on trunk
Fa0/21    1-4094
Fa0/22    1-4094
Fa0/23    1-4094
Fa0/24    1-4094
Port      Vlans allowed and active in management domain
Fa0/21    1,10,20,30,40,89
Fa0/22    1,10,20,30,40,89
Fa0/23    1,10,20,30,40,89
Fa0/24    1,10,20,30,40,89
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/21    10,40,89
Fa0/22    10,20,30,40,89
Fa0/23    30,40,89
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,10,30,40,89
```

```
SW1#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   vlan10_192_168_100_160_28         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
20   vlan20_192_168_100_128_27         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
30   vlan30_192_168_100_64_26          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
40   vlan40_192_168_100_0_26           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19
89   vlan89_192_168_100_240_28         active    Fa0/20
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

```
SW1#show spanning-tree
VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    4097
         Address     000f.248e.86c0
         Cost        19
         Port        24 (FastEthernet0/24)
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    12289  (priority 12288 sys-id-ext 1)
         Address     000d.29d8.fc00
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Altn BLK 19        48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Root FWD 19        16.24   P2p

VLAN0010
 Spanning tree enabled protocol ieee
 Root ID    Priority    4106
         Address     000f.248e.86c0
         Cost        19
         Port        24 (FastEthernet0/24)
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    8202   (priority 8192 sys-id-ext 10)
         Address     000d.29d8.fc00
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19        64.21   P2p
Fa0/22          Desg FWD 19        48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Root FWD 19        16.24   P2p

VLAN0020
 Spanning tree enabled protocol ieee
 Root ID    Priority    4116
         Address     000f.248e.8000
         Cost        19
         Port        22 (FastEthernet0/22)
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
         Address     000d.29d8.fc00
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Root FWD 19        48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Altn BLK 19        16.24   P2p
```

```
VLAN0030
 Spanning tree enabled protocol ieee
 Root ID    Priority    4126
          Address     000f.248e.8000
          Cost        19
          Port        22 (FastEthernet0/22)
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    8222   (priority 8192 sys-id-ext 30)
          Address     000d.29d8.fc00
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5           Desg FWD 19        128.5    Shr
Fa0/21          Altn BLK 19        64.21    P2p
Fa0/22          Root FWD 19        48.22    P2p
Fa0/23          Desg FWD 19        32.23    P2p
Fa0/24          Desg FWD 19        16.24    P2p

VLAN0040
 Spanning tree enabled protocol ieee
 Root ID    Priority    4136
          Address     000d.29d8.fc00
          This bridge is the root
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    4136   (priority 4096 sys-id-ext 40)
          Address     000d.29d8.fc00
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19        64.21    P2p
Fa0/22          Desg FWD 19        48.22    P2p
Fa0/23          Desg FWD 19        32.23    P2p
Fa0/24          Desg FWD 19        16.24    P2p

VLAN0089
 Spanning tree enabled protocol ieee
 Root ID    Priority    32857
          Address     000d.29d8.fc00
          This bridge is the root
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
          Address     000d.29d8.fc00
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19        64.21    P2p
Fa0/22          Desg FWD 19        48.22    P2p
Fa0/23          Desg FWD 19        32.23    P2p
Fa0/24          Desg FWD 19        16.24    P2p
```

2. CONFIGURACIÓN DEL SWITCH 2

```
SW2#sh running-config
Building configuration...
Current configuration : 1938 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW2
!
ip subnet-zero
!
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1,10 priority 4096
spanning-tree vlan 20,40 priority 8192
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access

……<resultado omitido>……..
interface FastEthernet0/21
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 64
interface FastEthernet0/22
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 48
interface FastEthernet0/23
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 32
interface FastEthernet0/24
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 16
interface GigabitEthernet0/1
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
```

```
 no ip route-cache
 shutdown
!
interface Vlan89
ip address 192.168.100.242 255.255.255.240
 no ip route-cache
!
ip http server
!
line con 0
line vty 5 15
!
end
```

```
SW2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 9
Maximum VLANs supported locally : 250
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xAE 0x61 0x12 0x21 0x92 0x15 0x32 0x8F
Configuration last modified by 192.168.100.241 at 3-1-93 00:35:09
```

```
SW2#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/21    on        802.1q         trunking    89
Fa0/22    on        802.1q         trunking    89
Fa0/23    on        802.1q         trunking    89
Fa0/24    on        802.1q         trunking    89
Port      Vlans allowed on trunk
Fa0/21    1-4094
Fa0/22    1-4094
Fa0/23    1-4094
Fa0/24    1-4094

Port      Vlans allowed and active in management domain
Fa0/21    1,10,20,30,40,89
Fa0/22    1,10,20,30,40,89
Fa0/23    1,10,20,30,40,89
Fa0/24    1,10,20,30,40,89
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/21    1,10,40
Fa0/22    1,10,20,30,40
Fa0/23    1,10,20
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,10,20,40,89

Fa0/21          Desg FWD 19      64.21  P2p
Fa0/22          Desg FWD 19      48.22  P2p
Fa0/23          Desg FWD 19      32.23  P2p
Fa0/24          Desg FWD 19      16.24  P2p
```

```
SW2#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1, Gi0/2
10   vlan10_192_168_100_160_28         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
20   vlan20_192_168_100_128_27         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
30   vlan30_192_168_100_64_26          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
40   vlan40_192_168_100_0_26           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19
89   vlan89_192_168_100_240_28         active    Fa0/20
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

```
SW2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000f.248e.86c0
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     000f.248e.86c0
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg FWD 19        64.21    P2p
Fa0/22           Desg FWD 19        48.22    P2p
Fa0/23           Desg FWD 19        32.23    P2p
Fa0/24           Desg FWD 19        16.24    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     000f.248e.86c0
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
             Address     000f.248e.86c0
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     000f.248e.8000
             Cost        19
             Port        22 (FastEthernet0/22)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    8212   (priority 8192 sys-id-ext 20)
             Address     000f.248e.86c0
```

```
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Root FWD 19         48.22   P2p
Fa0/23          Desg FWD 19         32.23   P2p
Fa0/24          Desg FWD 19         16.24   P2p

VLAN0030
 Spanning tree enabled protocol ieee
 Root ID    Priority    4126
        Address     000f.248e.8000
        Cost        19
        Port        22 (FastEthernet0/22)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
        Address     000f.248e.86c0
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/10          Desg FWD 19         128.10   P2p
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Root FWD 19         48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Altn BLK 19        16.24   P2p

VLAN0040
 Spanning tree enabled protocol ieee
 Root ID    Priority    4136
        Address     000d.29d8.fc00
        Cost        19
        Port        24 (FastEthernet0/24)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    8232   (priority 8192 sys-id-ext 40)
        Address     000f.248e.86c0
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19         64.21   P2p
Fa0/22          Desg FWD 19         48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Root FWD 19         16.24   P2p

VLAN0089
 Spanning tree enabled protocol ieee
 Root ID    Priority    32857
        Address     000d.29d8.fc00
        Cost        19
        Port        24 (FastEthernet0/24)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
        Address     000f.248e.86c0
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
          Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Altn BLK 19        48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Root FWD 19          16.24   P2p
```

3. CONFIGURACIÓN DEL SWITCH 3

```
SW3#show running-config
Building configuration...
Current configuration : 2204 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW3
!
ip subnet-zero
!
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain cisco2
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1 priority 8192
spanning-tree vlan 20,30 priority 4096
!
vlan 10
 name vlan10_192_168_100_160_28
vlan 20
 name vlan20_192_168_100_128_27
vlan 30
 name vlan30_192_168_100_64_26
vlan 40
 name vlan40_192_168_100_0_26
vlan 89
 name vlan89_192_168_100_240_28
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
……<resultado omitido>……..
```

```
interface FastEthernet0/21
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 64
interface FastEthernet0/22
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 48
interface FastEthernet0/23
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 32
interface FastEthernet0/24
 switchport trunk native vlan 89
 switchport mode trunk
 spanning-tree port-priority 16
interface GigabitEthernet0/1
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan89
 ip address 192.168.100.243 255.255.255.240
 no ip route-cache
ip http server
!
line con 0
line vty 5 15
!
end
```

```
SW3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 250
Number of existing VLANs        : 10
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xAE 0x61 0x12 0x21 0x92 0x15 0x32 0x8F
Configuration last modified by 192.168.100.241 at 3-1-93 00:35:09
```

```
SW3#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/21    on        802.1q         trunking    89
Fa0/22    on        802.1q         trunking    89
Fa0/23    on        802.1q         trunking    89
Fa0/24    on        802.1q         trunking    89
Port      Vlans allowed on trunk
Fa0/21    1-4094
Fa0/22    1-4094
Fa0/23    1-4094
Fa0/24    1-4094
Port      Vlans allowed and active in management domain
Fa0/21    1,10,20,30,40,89
Fa0/22    1,10,20,30,40,89
Fa0/23    1,10,20,30,40,89
Fa0/24    1,10,20,30,40,89
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/21    1,20,30
Fa0/22    1,20,30,40,89
Fa0/23    20,30,89
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,10,20,30,89
```

```
SW3#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1, Gi0/2
10   vlan10_192_168_100_160_28         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
20   vlan20_192_168_100_128_27         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
30   vlan30_192_168_100_64_26          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
40   vlan40_192_168_100_0_26           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19
89   vlan89_192_168_100_240_28         active    Fa0/20
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

```
SW3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000f.248e.86c0
             Cost        19
             Port        24 (FastEthernet0/24)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    8193   (priority 8192 sys-id-ext 1)
             Address     000f.248e.8000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Desg FWD 19        64.21    P2p
```

```
Fa0/22          Desg FWD 19       48.22   P2p
Fa0/23          Altn BLK 19       32.23   P2p
Fa0/24          Root FWD 19       16.24   P2p
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     000f.248e.86c0
             Cost        19
             Port        24 (FastEthernet0/24)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000f.248e.8000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19       64.21   P2p
Fa0/22          Altn BLK 19       48.22   P2p
Fa0/23          Altn BLK 19       32.23   P2p
Fa0/24          Root FWD 19       16.24   P2p
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     000f.248e.8000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4116   (priority 4096 sys-id-ext 20)
             Address     000f.248e.8000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19       64.21   P2p
Fa0/22          Desg FWD 19       48.22   P2p
Fa0/23          Desg FWD 19       32.23   P2p
Fa0/24          Desg FWD 19       16.24   P2p
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    4126
             Address     000f.248e.8000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4126   (priority 4096 sys-id-ext 30)
             Address     000f.248e.8000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Desg FWD 19       64.21   P2p
Fa0/22          Desg FWD 19       48.22   P2p
Fa0/23          Desg FWD 19       32.23   P2p
Fa0/24          Desg FWD 19       16.24   P2p
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    4136
```

```
        Address     000d.29d8.fc00
        Cost        19
        Port        22 (FastEthernet0/22)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
        Address     000f.248e.8000
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Root FWD 19          48.22   P2p
Fa0/23          Altn BLK 19        32.23   P2p
Fa0/24          Altn BLK 19        16.24   P2p
VLAN0089
  Spanning tree enabled protocol ieee
  Root ID    Priority    32857
        Address     000d.29d8.fc00
        Cost        19
        Port        22 (FastEthernet0/22)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
        Address     000f.248e.8000
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21          Altn BLK 19        64.21   P2p
Fa0/22          Root FWD 19          48.22   P2p
Fa0/23          Desg FWD 19          32.23   P2p
Fa0/24          Desg FWD 19          16.24   P2p
```

OBSERVACIONES

LABORATORIO N° 6 - IMPLEMENTACION DE INTERVLAN

DESCRIPCIÓN

El enrutamiento entre Vlan permite comunicar dominios de broadcast que representan áreas de trabajo, con la finalidad de transferir información de diferente índole entre las Vlan, así como también, comunicarlas con Internet u otras redes.

Como se sabe, los routers presentan un número limitado de puertos FastEthernet, por lo que no sería viable considerar el uso de un puerto por Vlan para su enrutamiento, en estos casos se convierte un puerto del router en una especie de puerto troncal creando una subinterfaz y asociándola a las Vlan.

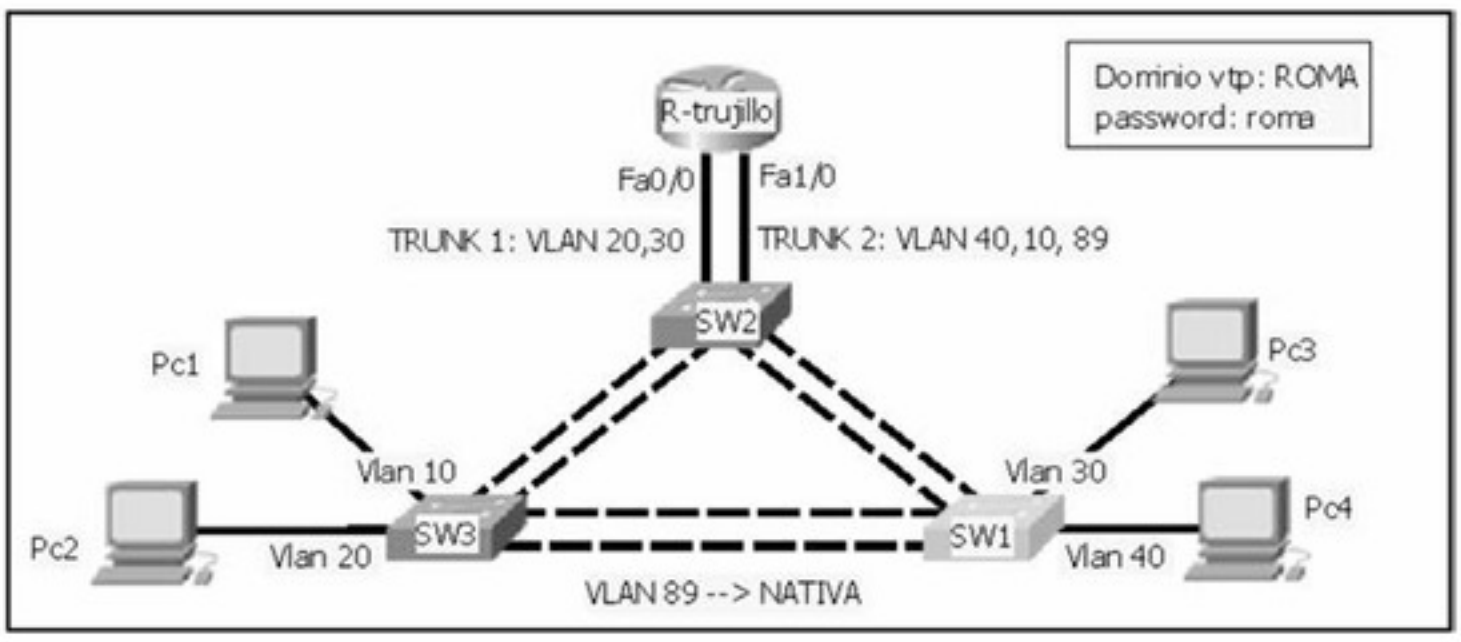
En el caso de filtrar la comunicación entre una Vlan con otra, pueden emplearse listas de control de acceso.

OBJETIVOS

- Implementar el enrutamiento entre las Vlan en conjunto con VTP y STP.
- Reforzar los conocimientos respecto al dominio VTP y spanning tree.

PLANTEAMIENTO

- Implementar el siguiente esquema para el enrutamiento de redes virtuales, considerando, para este caso, que el router R-trujillo empleará dos interfaces como enlaces troncales para permitir el enrutamiento, como una forma de equilibrar el tráfico por cada interfaz.



- Considerar la siguiente cantidad de Host por Vlan:

Lan	10	20	30	40	89
Host	60	20	120	80	10

- El dominio VTP deberá tener las siguientes características:

SW1	Server
SW2	Cliente1
SW3	Transparente

- SPANNING TREE:

VLAN	Root Primary	Root Secondary
1	SW2	SW3
10	SW2	SW1
20	SW3	SW2
30	SW3	SW1
40	SW1	SW2

SOLUCIÓN

En el presente laboratorio excluiremos la configuración de algunas opciones por tenerse en los laboratorios anteriores configuraciones y pautas similares. Se brindará mayor énfasis a la configuración de enrutamiento entre Vlan.

FASE 1:

1. Realizar la eliminación de cualquier configuración anterior en cada uno de los equipos para facilitar su nueva configuración.
2. Configure las opciones básicas de cada equipo; recuerde siempre tener un servidor TFTP para alojar una copia del IOS y del archivo de configuración.

FASE 2:

1. A continuación, la tabla resumen sobre el direccionamiento IP desarrollado:

Vlan	Host	ID red	Máscara de subred
10	60	172.16.1.0	255.255.255.192
20	20	172.16.1.64	255.255.255.224
30	120	172.16.0.0	255.255.255.128
40	80	172.16.0.128	255.255.255.128
89	10	172.16.1.96	255.255.255.240

2. Se muestra la distribución de direcciones:

Dispositivos	Interfaz	Vlan	Dirección IP	Puerta de enlace
Router	F0/0.1	20	172.16.1.65 /27	------
	F0/0.2	30	172.16.0.1 /25	------
	F1/0.1	10	172.16.1.1 /26	------
	F1/0.2	40	172.16.0.129 /25	------
	F1/0.3	89	172.16.1.97 /28	------
Switch 1	Vlan 89	89	172.16.1.101 /28	172.16.1.97
Switch 2	Vlan 89	89	172.16.1.102 /28	172.16.1.97
Switch 3	Vlan 89	89	172.16.1.103 /28	172.16.1.97
PC 1	NIC	10	172.16.1.2 /26	172.16.1.1
PC 2	NIC	20	172.16.1.66 /27	172.16.1.65
PC 3	NIC	30	172.16.0.1 /25	172.16.0.1
PC 4	NIC	40	172.16.0.130 /25	172.16.0.129

FASE 3:

1. Considere como referencia los laboratorios anteriores para la implementación del dominio VTP, Vlan y la configuración del spanning tree.
2. La configuración del switch 2 en sus puertos troncales con conexión al router R-trujillo no requiere de nada especial, simplemente que sean troncales.
3. Si desea, puede acceder a cada puerto troncal en el switch 2 e indicar las Vlan que alojará cada uno.
4. Agregar en la configuración de los switches la dirección del Gateway o puerta de enlace. Todos los switches tendrán la misma dirección ya que se encuentran en la misma Vlan; en este caso, vendría a ser la dirección de la subinterfaz a colocarse en el router.

```
SW-3#config ter
SW-3#(config)# ip default-gateway 172.16.1.97
```

5. Realizar la comprobación de la configuración entre los switches y las PC, con pruebas de conectividad y acceso por Telnet; recuerde también que aún no habrá conectividad entre Vlan ya que falta el enrutamiento.

FASE 4: Enrutamiento

1. A continuación se desarrollará la configuración del router, para la cual se crearán subinterfaces que permitan transferir tramas de las Vlan 20 y 30 por la interfaz FastEthernet 0/0, y para las Vlan 10, 40 y 89, por la interfaz FastEthernet 1/0.
2. Tener presente que ciertos modelos de router no soportan encapsulamiento, ya sea por limitación de IOS o de la propia arquitectura.
3. La configuración de subinterfaces debe considerar el encapsulamiento dot1q e identificar las tramas con un número de etiqueta de acuerdo al número de Vlan. Después de ello coloque su dirección IP (véase el ejemplo).

```
R-trujillo(config-if)#int f0/0.1
R-trujillo(config-subif)#encapsulation dot1Q 20
R-trujillo(config-subif)#ip address 172.16.1.65 255.255.255.224
```

4. Si se realiza la configuración al contrario, es decir, considerando primero la dirección IP, se mostrará un mensaje, como se aprecia a continuación, indicando que deberá definir antes el encapsulamiento en IEEE 802.10, IEEE 802.1Q o ISL vLAN.

```
R-trujillo(config)#int f0/0.5
R-trujillo(config-subif)#ip address 192.168.1.1 255.255.255.0
% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

R-trujillo(config-subif)#
```

5. A continuación se muestra la configuración completa desarrollada en el router:
   - Según la configuración realizada, se ha creado, para la Vlan 20, la subinterfaz FastEthernet0/0.1 y en el encapsulamiento para establecer la relación con la Vlan 20 se coloca el valor de 20, que viene a ser el ID de la Vlan.

- Tome como referencia los comandos que continúan en la configuración de las subinterfaces para las otras Vlan.
- En el caso de la Vlan 89, se ha creado la subinterfaz FastEthernet 1/0.3 con encapsulamiento **dot1q** y el ID 89 para relacionar a la Vlan. A su vez, se coloca **native**, indicándole al router que será la **Vlan nativa** y por lo tanto sus tramas ingresarán sin etiquetas.

```
R-trujillo#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R-trujillo(config)#int f0/0
R-trujillo(config-if)#no shut
R-trujillo(config-if)#int f0/0.1
R-trujillo(config-subif)#encapsulation dot1Q 20
R-trujillo(config-subif)#ip address 172.16.1.65 255.255.255.224
R-trujillo(config-subif)#int f0/0.2
R-trujillo(config-subif)#encapsulation dot1Q 30
R-trujillo(config-subif)#ip address 172.16.0.1 255.255.255.128
R-trujillo(config-subif)#exit
R-trujillo(config)#int f1/0
R-trujillo(config-if)#no shut
R-trujillo(config-if)#int f1/0.1
R-trujillo(config-subif)#encapsulation dot1Q 10
R-trujillo(config-subif)#ip address 172.16.1.1 255.255.255.192
R-trujillo(config-subif)#int f1/0.2
R-trujillo(config-subif)#encapsulation dot1Q 40
R-trujillo(config-subif)#ip address 172.16.0.129 255.255.255.128
R-trujillo(config-subif)#int f1/0.3
R-trujillo(config-subif)#encapsulation dot1Q 89 native
R-trujillo(config-subif)#ip address 172.16.1.97 255.255.255.240
R-trujillo(config-subif)#exit
R-trujillo(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
R-trujillo#wr
Building configuration...
[OK]
R-trujillo#
```

6. El router no necesita habilitar un enrutamiento dinámico ni estático, ya que para el router son redes directamente conectadas y por lo tanto el enrutamiento es automático. Sólo necesita que las interfaces estén activadas.

```
R-trujillo#sh ip route
…….. < RESULTADO OMITIDO >……
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 4 masks
C       172.16.0.0/25 is directly connected, FastEthernet0/0.2
C       172.16.0.128/25 is directly connected, FastEthernet1/0.2
C       172.16.1.0/26 is directly connected, FastEthernet1/0.1
C       172.16.1.64/27 is directly connected, FastEthernet0/0.1
C       172.16.1.96/28 is directly connected, FastEthernet1/0.3
R-trujillo#
```

7. En el router no se podrá configurar para que ambas interfaces FastEthernet pertenezcan a todas las Vlan y así permitir que las tramas de cada Vlan circulen por las dos interfaces, ya que para eso deberá haber subinterfaces en ambos puertos para todas las Vlan, así como direcciones IP para cada una, lo cual no es permitido por el router, mostrando mensajes de error.

```
R-trujillo(config-subif)#encapsulation dot1Q 20
%Configuration of multiple subinterfaces of the same main
interface with the same VID (20) is not permitted.
This VID is already configured on FastEthernet0/0.1.
```

FASE 5: Prueba

1. Realizar el diagnóstico respectivo entre Host de diferentes Vlan. Es posible que inicialmente tarde en lograr conectividad pero luego deberá realizarse sin problemas.
2. Capture la información configurada, así como el resultado de diversos comandos, como las Vlan, el dominio VTP, la configuración STP y la tabla de enrutamiento.

CONFIGURACIÓN FINAL DE CADA EQUIPO

1. Configuración final del SWITCH 3

```
SW-3#sh runn
Building configuration...
Current configuration : 1309 bytes
!
version 12.1
no service password-encryption
!
hostname SW-3
!
spanning-tree vlan 20 priority 24576
spanning-tree vlan 10,30 priority 28672
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/5
```

```
 switchport access vlan 20
!
interface FastEthernet0/6
 switchport access vlan 10
!
…….. < RESULTADO OMITIDO >……
!
interface Vlan89
 ip address 172.16.1.103 255.255.255.240
!
ip default-gateway 172.16.1.97
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

```
SW-3#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   RR.HH-OTROS                      active    Fa0/6
20   ADMINISTRATIVOS                  active    Fa0/5
30   EMPLEADOS-1                      active
40   EMPLEADOS-2                      active
89   SOPORTE                          active

…….. < RESULTADO OMITIDO >……
```

```
SW-3#show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : ROMA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8D 0xCF 0xBA 0x6F 0xD9 0xDD 0xF6 0x73
Configuration last modified by 0.0.0.0 at 3-1-93 00:21:49
```

```
SW-3#show spanning-tree
VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    24616
         Address     0000.0CBE.A5E8
         Cost        19
         Port        8(FastEthernet0/8)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
         Address     0001.C726.7BEA
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Root FWD 19        128.8    P2p


VLAN0010
 Spanning tree enabled protocol ieee
 Root ID    Priority    24586
         Address     0000.0CBE.A5E8
         Cost        19
         Port        2(FastEthernet0/2)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
         Address     0001.C726.7BEA
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/6            Desg FWD 19        128.6    P2p


VLAN0020
 Spanning tree enabled protocol ieee
 Root ID    Priority    24596
         Address     0001.C726.7BEA
         This bridge is the root
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
         Address     0001.C726.7BEA
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00D0.BA52.951D

             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     0001.C726.7BEA
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p


VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     0000.0CBE.A5E8
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     0001.C726.7BEA
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p


VLAN0089
  Spanning tree enabled protocol ieee
  Root ID    Priority    24665
             Address     00D0.BA52.951D
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
             Address     0001.C726.7BEA
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
```

2. Configuración final del SWITCH 2

```
SW-2#sh runn
Building configuration...
Current configuration : 1578 bytes
!
version 12.1
no service password-encryption
!
hostname SW-2
!
vtp domain ROMA
vtp mode transparent
vtp password roma
vtp version 2
!
spanning-tree vlan 10,40 priority 24576
spanning-tree vlan 89 priority 28672
!
vlan 10
 name RR.HH-OTROS
!
vlan 20
 name ADMINISTRATIVOS
!
vlan 30
 name EMPLEADOS-1
!
vlan 40
 name EMPLEADOS-2
!
vlan 89
 name SOPORTE
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk native vlan 89
```

```
 switchport mode trunk
!
…….. < RESULTADO OMITIDO >……
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan89
 ip address 172.16.1.102 255.255.255.240
!
ip default-gateway 172.16.1.97
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

```
SW-2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     0000.0CBE.A5E8
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0000.0CBE.A5E8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0000.0CBE.A5E8
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0000.0CBE.A5E8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0001.C726.7BEA
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0000.0CBE.A5E8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p


VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     00D0.BA52.951D
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0000.0CBE.A5E8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

```
VLAN0040
 Spanning tree enabled protocol ieee
 Root ID    Priority    24616
          Address     0000.0CBE.A5E8
          This bridge is the root
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    24616  (priority 24576 sys-id-ext 40)
          Address     0000.0CBE.A5E8
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Desg FWD 19        128.1    P2p
Fa0/2           Desg FWD 19        128.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/4           Desg FWD 19        128.4    P2p
Fa0/5           Desg FWD 19        128.5    P2p
Fa0/6           Desg FWD 19        128.6    P2p


VLAN0089
 Spanning tree enabled protocol ieee
 Root ID    Priority    24665
          Address     00D0.BA52.951D
          Cost        19
          Port        2(FastEthernet0/2)
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    28761  (priority 28672 sys-id-ext 89)
          Address     0000.0CBE.A5E8
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Desg FWD 19        128.1    P2p
Fa0/2           Root FWD 19        128.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/4           Altn BLK 19        128.4    P2p
Fa0/5           Desg FWD 19        128.5    P2p
Fa0/6           Desg FWD 19        128.6    P2p
```

```
SW-2#
SW-2# SH VTP STatus
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Transparent
VTP Domain Name                 : ROMA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF1 0xAE 0xE6 0x30 0xD6 0x46 0xB9 0xC5
Configuration last modified by 0.0.0.0 at 3-1-93 00:15:18
```

```
SW-2#SHOW VLAN BRIEF
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                            Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                            Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                            Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                            Fa0/23, Fa0/24
10   RR.HH-OTROS                  active
20   ADMINISTRATIVOS              active
30   EMPLEADOS-1                  active
40   EMPLEADOS-2                  active
89   SOPORTE                      active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

```
SW-2#SH INTERfaces TRUNk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      89
Fa0/2       on           802.1q         trunking      89
Fa0/3       on           802.1q         trunking      89
Fa0/4       on           802.1q         trunking      89
Fa0/5       on           802.1q         trunking      89
Fa0/6       on           802.1q         trunking      89
Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
Fa0/4       1-1005
Fa0/5       1-1005
Fa0/6       1-1005
```

4. Configuración final del SWITCH 1

```
SW-1#Show running-config
Building configuration...
Current configuration : 1312 bytes
!
version 12.1
no service password-encryption
!
hostname SW-1
!
spanning-tree vlan 30,89 priority 24576
spanning-tree vlan 20,40 priority 28672
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/2
```

```
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
 switchport access vlan 40
!
…….. < RESULTADO OMITIDO >……
!
interface Vlan89
 ip address 172.16.1.101 255.255.255.240
!
ip default-gateway 172.16.1.97
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

```
SW-1#show vlan brief
VLAN Name                    Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                 active    Fa0/2, Fa0/4, Fa0/6, Fa0/7
                                       Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                       Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                       Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                       Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   RR.HH-OTROS             active
20   ADMINISTRATIVOS         active
30   EMPLEADOS-1             active    Fa0/5
40   EMPLEADOS-2             active    Fa0/8
89   SOPORTE                 active
1002 fddi-default            active
1003 token-ring-default      active
1004 fddinet-default         active
1005 trnet-default           active
```

```
SW-1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : ROMA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8D 0xCF 0xBA 0x6F 0xD9 0xDD 0xF6 0x73
Configuration last modified by 0.0.0.0 at 3-1-93 00:21:49
Local updater ID is 172.16.1.101 on interface Vl89 (lowest numbered VLAN interface found)
```

```
SW-1#
SW-1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24616
             Address     0000.0CBE.A5E8
             Cost        19
             Port        7(FastEthernet0/7)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.BA52.951D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Root FWD 19        128.7    P2p


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0000.0CBE.A5E8
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00D0.BA52.951D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
```

```
VLAN0020
 Spanning tree enabled protocol ieee
 Root ID    Priority    24596
         Address     0001.C726.7BEA
         Cost        19
         Port        1(FastEthernet0/1)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Root FWD 19        128.1    P2p
Fa0/3           Altn BLK 19        128.3    P2p


VLAN0030
 Spanning tree enabled protocol ieee
 Root ID    Priority    24606
         Address     00D0.BA52.951D
         This bridge is the root
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    24606  (priority 24576 sys-id-ext 30)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Desg FWD 19        128.1    P2p
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/5           Desg FWD 19        128.5    P2p


VLAN0040
 Spanning tree enabled protocol ieee
 Root ID    Priority    24616
         Address     0000.0CBE.A5E8
         Cost        19
         Port        1(FastEthernet0/1)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    28712  (priority 28672 sys-id-ext 40)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Root FWD 19        128.1    P2p
Fa0/3           Altn BLK 19        128.3    P2p
Fa0/8           Desg FWD 19        128.8    P2p
```

```
VLAN0089
 Spanning tree enabled protocol ieee
 Root ID    Priority    24665
          Address     00D0.BA52.951D
          This bridge is the root
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    24665  (priority 24576 sys-id-ext 89)
          Address     00D0.BA52.951D
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1           Desg FWD 19        128.1    P2p
Fa0/3           Desg FWD 19        128.3    P2p
```

6. Configuración final del router R-trujillo

```
R-trujillo#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 4 masks
C       172.16.0.0/25 is directly connected, FastEthernet0/0.2
C       172.16.0.128/25 is directly connected, FastEthernet1/0.2
C       172.16.1.0/26 is directly connected, FastEthernet1/0.1
C       172.16.1.64/27 is directly connected, FastEthernet0/0.1
C       172.16.1.96/28 is directly connected, FastEthernet1/0.3
R-trujillo#
```

```
R-trujillo#sh runn
Building configuration...
Current configuration : 1110 bytes
!
version 12.2
no service password-encryption
!
hostname R-trujillo
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/0.1
 encapsulation dot1Q 20
 ip address 172.16.1.65 255.255.255.224
!
interface FastEthernet0/0.2
 encapsulation dot1Q 30
 ip address 172.16.0.1 255.255.255.128
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0.1
 encapsulation dot1Q 10
 ip address 172.16.1.1 255.255.255.192
!
interface FastEthernet1/0.2
 encapsulation dot1Q 40
 ip address 172.16.0.129 255.255.255.128
!
interface FastEthernet1/0.3
 encapsulation dot1Q 89
 ip address 172.16.1.97 255.255.255.240
!
…….. < RESULTADO OMITIDO >……
!
line con 0
line vty 0 4
 password class
 login
line vty 5
 password class
 login
!
end
```

OBSERVACIONES

ROUTING

Se refiere al mecanismo de operación en los routers, describiéndose su configuración básica, el respaldo de archivos, la recuperación del IOS, la implementación de las diferentes características en el enrutamiento estático, el enrutamiento con los protocolos OSPF, RIP y EIGRP, así como también el diagnóstico de conexiones y la solución de problemas.

Considerando los laboratorios iniciales se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo.

LABORATORIO N° 1: Instalación del IOS en el router

Se realiza la comprobación del estado de la imagen del IOS, indicándose paso a paso el orden para restablecer la imagen del sistema operativo. La primera opción es mediante el puerto consola, el emulador HyperTerminal y el protocolo XMODEM. La segunda opción es vía red, con el empleo del servidor TFTP.

LABORATORIO N° 2: CONFIGURACIÓN BÁSICA DEL ROUTER

Se implementan las opciones de configuración básica, como el nombre del equipo, la contraseña de acceso, la tabla Host, y se comprueba el funcionamiento del router mediante las pruebas de rutina.

LABORATORIO N° 3: Diagnóstico de conexiones I

En una implementación topológica de malla parcial con enrutamiento RIP, se emplean los comandos para el diagnóstico de conexiones. Está dividido en cuatro fases donde se revisa la diferencia entre una conexión física y el enrutamiento, mediante el uso de los protocolos CDP, ICMP y TELNET.

LABORATORIO N° 4: Diagnóstico de conexiones II

Es un laboratorio de topología con tres routers conectados uno al otro formando un anillo, donde se realiza el diagnóstico de conexiones mediante el análisis de fallas con la aplicación de herramientas de conectividad. La finalidad es tener un criterio ordenado para actuar, de acuerdo a ciertas circunstancias, basándose en el modelo de capas.

LABORATORIO N° 5: RIP Y LAS RUTAS DE RESPALDO

Se analiza el comportamiento del protocolo de enrutamiento dinámico RIP versión 2, desde su configuración básica de enrutamiento, siguiendo con el diagnóstico de tablas, la comprobación de su base de datos de rutas, la verificación de sus temporizadores y el uso de una ruta de respaldo con el empleo de rutas estáticas (ruta backup).

LABORATORIO N° 6: Redistribución de rutas estáticas en RIP

El laboratorio está dividido en dos casos. En el primer caso se muestra una topología donde al enrutamiento RIP se suma por un lado la ruta por defecto con enlace hacia Internet y por el otro, la conexión de otro router hacia una sucursal mediante una ruta estática. En el segundo caso un mismo router tiene conexión hacia una sucursal y a Internet, y redistribuye sus rutas hacia su enrutamiento dinámico.

LABORATORIO N° 7: EIGRP con rutas de distinto ancho de banda

La topología permite comprobar el funcionamiento de EIGRP, desde su configuración básica hasta la operación del algoritmo DUAL. Se tienen enlaces de distinto ancho de banda donde se demuestra cómo funcionan las rutas de respaldo al caer el enlace.

LABORATORIO N° 8: EIGRP (análisis de DUAL)

El esquema de red facilita el diagnóstico de vecinos EIGRP, de las tablas de enrutamiento en la topología y un análisis detallado, mediante ejemplos, del cálculo que realiza el algoritmo DUAL para la obtención de las tablas topológicas.

LABORATORIO N° 9: EIGRP y redistribución de rutas estáticas

Se plantea una topología con cuatro routers enrutados con EIGRP, donde en uno de ellos se configura la redistribución de una ruta por defecto y en otro router, la ruta estática. Así mismo, se configura el resumen y publicación de rutas.

LABORATORIO N° 10: ENRUTAMIENTO OSPF

Se presenta la configuración del protocolo OSPF en una sola área en una topología mixta con enlaces punto a punto y multiacceso. Se realiza la redistribución de la ruta por defecto dentro del proceso OSPF, análisis de costo, la definición del DR y BDR en la red multiacceso, y la optimización con los temporizadores.

LABORATORIO N° 11: ENRUTAMIENTO OSPF - OPCIONES AVANZADAS

Es un laboratorio que difiere en topología del anterior. Se configura el protocolo OSPF en forma básica, comprobando las tablas de operación (vecino, enrutamiento y topológica) y una configuración avanzada redistribuyendo rutas estática y por defecto en diferentes routers. Así mismo, se establece el DR y BDR mediante la prioridad y la verificación de rutas internas y externas.

LABORATORIO N° 12: ENRUTAMIENTO OSPF CON RUTAS POR DEFECTO

En la topología se muestra una doble conexión hacia un ISP, donde se configuran rutas por defecto, pero con distinta distancia administrativa, para luego redistribuirlas dentro del proceso OSPF. La finalidad es tener un enlace principal y otro de respaldo.

Capítulo

2 Routing

LABORATORIO Nº 1 - Instalación del IOS en el router

DESCRIPCIÓN

El sistema operativo en un router es fundamental para su operación. Considerando los múltiples problemas que se presentan, existe la necesidad de conocer las alternativas de instalación, en caso haya sido borrado o esté dañado.

Existen dos formas de instalar el IOS hacia el router: una, mediante el servidor TFTP y la otra opción, mediante el protocolo Xmodem.

OBJETIVOS

- Instalar el IOS en el router mediante el protocolo Xmodem.
- Instalar el IOS en el router mediante el servidor TFTP.

PLANTEAMIENTO

1. **Comprobación en el router de la falta de IOS**

   En ciertos casos el router puede ser manipulado y presentar ciertos problemas que merecen ser descartados para comprobar si en realidad se requiere de la instalación del IOS:

Registro modificado:

- Verifique el registro de configuración, puede tener los valores modificados.
- Se digita el comando **confreg** y se mostrará el valor en números hexadecimales, que pudieran ser **0x2100**, por ejemplo, lo cual indica que no cargará el IOS desde la memoria Flash.
- Se deberá modificar, si este el caso, colocando el comando **confreg 0x2102** para indicar una carga normal del equipo, y luego colocar **reset** para restaurar el router.

IOS dañado:

- Desde el modo rommon se puede colocar el comando **dir flash** y observar si presenta o no el IOS en la memoria Flash.
- Si el IOS está presente puede significar que está dañado, que no corresponde al sistema de hardware o que han digitado mal el nombre del IOS con el comando boot.

- Descarte dicha opción colocando el comando boot seguido del nombre del IOS almacenado en la memoria Flash.

```
rommon 1 > dir flash:
      File size          Checksum   File name
  5571584 bytes (0x550400)   0x0455    c1700-adventerprisek9-mz.124-19.bin

rommon 2 >boot c1700-adventerprisek9-mz.124-19.bin
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco Systems, Inc.
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

boot of "c1700-adverterprise9-mz.124-19.bin" failed
error returned: File boot failed -- File not accessible
loadprog: error - on file open
boot: cannot load "c1700-adverterprise9-mz.124-19.bin"

Boot process failed...

The system is unable to boot automatically.  The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 >
```

IOS eliminado:

- Desde el modo rommon se puede colocar el comando **dir flash** y observar si presenta o no el IOS en la memoria Flash.
- Al no encontrarse sistema operativo se procede a instalarlo.

```
rommon 1 > dir flash:
      File size          Checksum   File name

rommon 2
```

2. Descarga de IOS mediante Xmodem en el modo rommon

Esta opción es una trasferencia mediante el puerto consola y es usada en casos de emergencia. Habida cuenta de que el puerto consola es de baja velocidad se prefiere modificar su velocidad al valor máximo soportado.

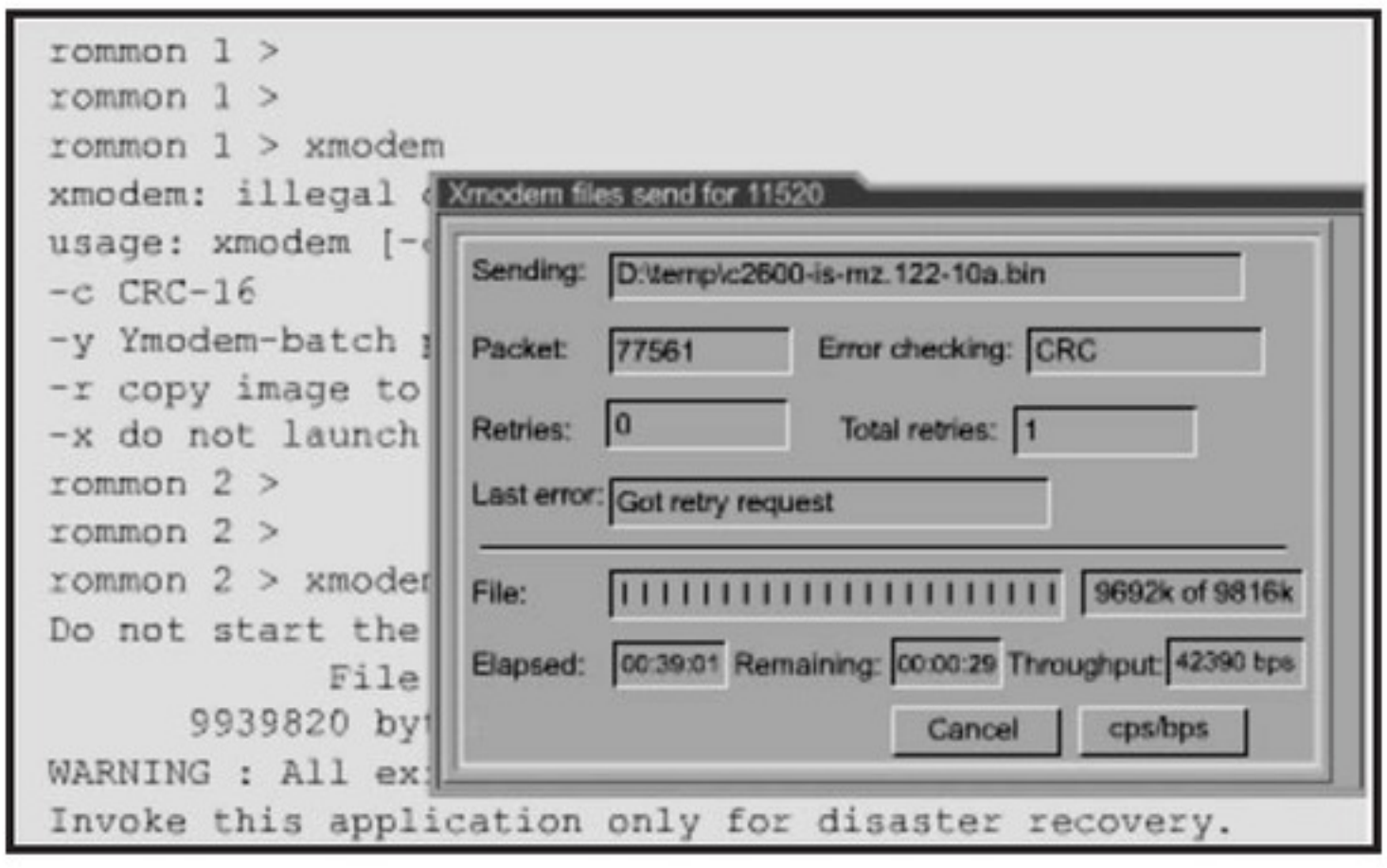
1. Al cargar en modo **rommon**, realizamos las pruebas respectivas.
2. **Modifique la velocidad de la consola**:
   a. Digite **"confreg"**.
   b. Cuando se le solicite "**change console baud rate**? y/n", marque *n*.
   c. Si selecciona *y* aparecerá un indicador para seleccionar la nueva velocidad.
   d. Digite "**115200**", como velocidad.
   e. Una vez que ha cambiado la velocidad de la consola, reinicie el router en el modo **rommon**.
   f. Se debe cerrar la sesión de 9600 e iniciar una nueva a 115200 bps.
3. **Restaurar la imagen del software IOS desde la PC**
   1. Digite el comando **xmodem -c*nombre_del_archivo***. Por ejemplo, para restaurar un archivo de imagen del IOS, de nombre "c2600-is-mz.122-10a.bin", ejecute el comando:

xmodem -c c2600-is-mz.122-10a.bin

2. La **-c** le indica al proceso Xmodem que debe usar Verificación de redundancia cíclica (CRC) para detectar errores durante la descarga.

```
    rommon 1 >
          rommon 1 >xmodem -?
          xmodem: illegal option -- ?
          usage: xmodem [-cyrx] <destination filename>
                -c  CRC-16
                -y  ymodem-batch protocol
                -r  copy image to dram for launch
                -x  do not launch on download completion
   rommon 2 >xmodem -c c2600-is-mz.122-10a.bin

 Do not start the sending program yet...

  Warning:  All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y
Ready to receive file c2600-is-mz.122-10a.bin ...
```

3. El router no inicia la transferencia de inmediato, sino que le muestra un mensaje de advertencia.
4. El mensaje le informa que la bootflash será borrada y le pregunta si desea continuar. Una vez que se acepta continuar, el router le indicará que puede iniciar la transferencia.
5. **Transferencia Xmodem desde el emulador de terminal**.
   - En HyperTerminal seleccione **Transfer** > **Send File** (Transferir > Enviar archivo).
   - Al aparecer la ventana **Send File** (Enviar archivo), indique el nombre y la ubicación de la imagen.
   - Seleccione Xmodem como el protocolo e inicie la transferencia.
   - La ventana Sending File (Enviando archivo) mostrará el estado de la transferencia.



6. Modifique el registro de configuración, de ser necesario.
7. Reinicie el router.

Descarga del IOS mediante el puerto LAN para conexión hacia un servidor TFTP

1. Empleando un equipo como servidor TFTP

i. Al cargar en modo rommon, realizamos las pruebas respectivas.

ii. Preparamos el router configurando el direccionamiento IP del puerto LAN para facilitar la transferencia de la imagen IOS.

iii. Fijar las variables de entorno necesarias para realizar una carga del IOS desde un servidor TFTP.

```
rommon 1 > IP_ADDRESS=192.168.7.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.7.25
rommon 4 > TFTP_SERVER=192.168.7.25
rommon 5>  TFTP_FILE=c1700-y-mz.122-2.XJ.BIN
```

iv. Verificar el estado de las variables.

```
rommon 6 > set
PS1=rommon ! >
TFTP_CHECKSUM=1
RET_2_RUTC=0
RET_2_RTS=
IP_SUBNET_MASK=255.255.255.0
TFTP_FILE=c1700-y-mz.122-2.XJ.BIN
BSI=0
IP_ADDRESS=192.168.7.1
DEFAULT_GATEWAY=192.168.7.25
TFTP_SERVER=192.168.7.25
```

v. Activar el servidor TFTP y contar con una imagen del IOS válida en el directorio, que éste utilizará para la carga (ver video o anexos).

vi. Ejecutar desde el rommon el comando **tftpdnld**, que iniciará la carga del IOS desde el servidor TFTP hacia el router.

vii. Este comando cargará el IOS en la RAM, borrará la Flash y copiará el IOS de la RAM a la Flash.

***Nota**: La conectividad entre el router y el servidor TFTP sólo se activa durante el proceso de transferencia del IOS.*

```
rommon 7 > tftpdnld

    IP_ADDRESS: 192.168.7.1
    IP_SUBNET_MASK: 255.255.255.0
    DEFAULT_GATEWAY: 192.168.7.25
    TFTP_SERVER: 192.168.7.25
    TFTP_FILE: c1700-y-mz.122-2.XJ.BIN

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:  y

Receiving c1700-y-mz.122-2.XJ.BIN from 192.168.7.25 !!!!!!!!!!!
!!!!!!!!!!
```

viii. Una vez cargado el IOS verificamos la copia en la Flash, para luego reiniciar el equipo:

```
rommon 9 > dir flash:
      File size          Checksum   File name
  3930812 bytes (0x3bfabc)   0x0265    c1700-y-mz.122-2.XJ.BIN
rommon 10 > reset
```

2. Empleando un router como servidor TFTP

- Esta alternativa es igual al caso anterior, con la única diferencia de que el servidor TFTP será otro router y debemos configurarlos en la misma red, así como conectarnos mediante un cable cruzado.
- Coloque los siguientes comandos:
  - o Router#configure terminal
  - o Router(config)#tftp-server flash:xxxxxxxx.bin
- Una vez completada la configuración, los pasos seguidos para copiar el IOS al router son los mismos.

OBSERVACIONES Y/O COMENTARIOS

_____

_____

_____

_____

LABORATORIO Nº 2 - CONFIGURACIÓN BÁSICA DEL ROUTER

DESCRIPCIÓN

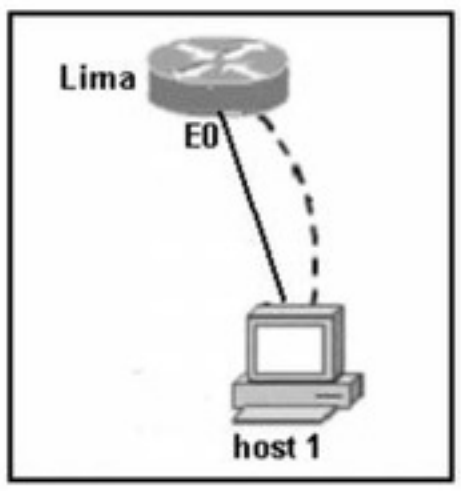
Dentro del manejo de equipos existen varias opciones básicas de configuración que se tienen que considerar y que facilitan el trabajo posterior de configuración.

Esta configuración básica brinda entre otras cosas la facilidad de administración, simplificando el trabajo de todo administrador, y brinda también la seguridad mínima para la protección del equipo.

OBJETIVOS

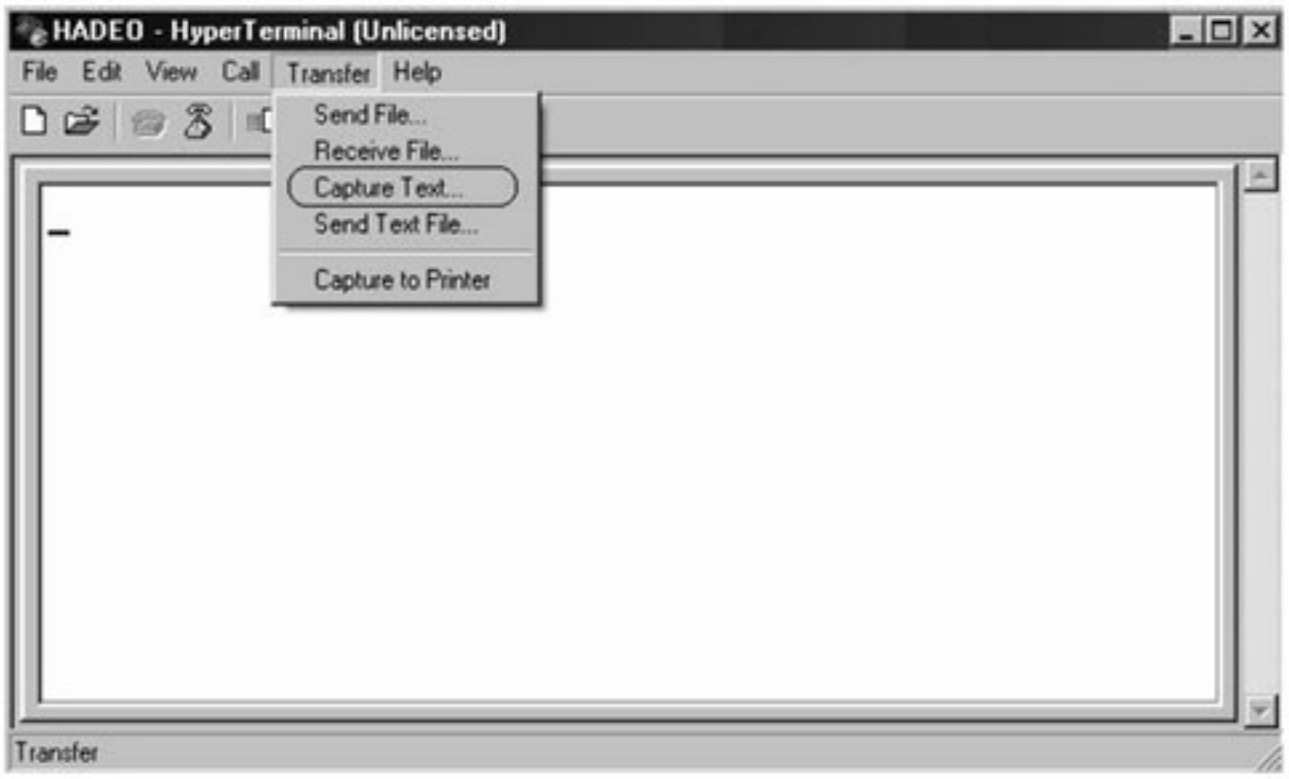
1. Implementar las opciones de configuración básica.
2. Comprobar el funcionamiento del router mediante las pruebas de rutina.

PLANTEAMIENTO



FASE I: PASOS PREVIOS:

1. Realizar la conexión, hacia el equipo, de todo el cableado y cargar el emulador en la PC para la administración del router.
2. Verifique el estado del router secuencialmente en su carga.
3. Borre la configuración del router, si la tuviera, y reinícielo.
4. Habilite la opción de captura de texto en el emulador.



FASE II: CONFIGURACIÓN BÁSICA

1. Es siempre recomendable tener una plantilla en un editor de texto ya que facilita la labor de configuración.
   - Desde dicha plantilla se puede copiar a la consola de configuración y corregir más fácilmente cualquier problema presentado.
   - Asimismo, si se tiene grabada una captura de texto se podrá pegar nuevamente a la configuración del router, sólo se deberán eliminar algunas sentencias.
2. **Contraseña para el puerto consola**
   - Es una contraseña de acceso general al router al momento de acceder en el modo usuario, para este caso la contraseña es cisco.
   - Considere que los caracteres de contraseña no aparecen al momento de ser digitados; además, se tiene un máximo de tres intentos para su aceptación.

```
Router>enable
Router#configure terminal
Router(config)#hostname Lima
Lima(config)# line console 0
Lima(config-line)# login
Lima(config-line)# password cisco
Lima(config-line)# ^Z
Lima# exit
User access verificación
Password : cisco
Lima>
```

3. **Contraseña para el modo privilegiado**
   - Es empleada por seguridad para este nivel de configuración, donde se tienen dos formas de realizarla: una, mediante el enable password ****** y la otra, mediante el enable secret *****.
   - El enable secret tiene prioridad sobre el enable password: visualiza el archivo de configuración que se está ejecutando actualmente en la RAM.

```
Lima(config)#enable password clase1
Lima(config)#exit
Lima>enable
Password : clase1

Lima# configure terminal
Lima(config)# enable secret clase2
Lima(config)# ^z
Lima# disable
Lima> enable
Password : cisco x
Password : clase2
Lima#
```

4. **Contraseña para el puerto auxiliar**
   - En ciertas ocasiones puede fallar el puerto consola, por un mal manejo, y el puerto auxiliar podría facilitar la configuración del router, por lo que se recomienda tener siempre colocada una contraseña en caso de emergencia.

- Cambiar la ubicación del cable consola para la prueba respectiva.

```
Lima(config)#  line aux 0
Lima(config-line)# login
Lima(config-line)# password cisco1
Lima(config-line)# ^Z
Lima# exit
```

5. **Contraseña para el acceso al terminal virtual** (para iniciar sesión vía Telnet)
   - El acceso al terminal virtual permite un máximo de cinco conexiones concurrentes (del 0 al 4), por lo que al momento de la habilitación se puede definir la cantidad máxima.
   - La configuración de acceso al terminal virtual se complementa con la contraseña del modo privilegiado. Adicionalmente a ello, la dirección IP está en uno o todos los puertos de conexión.
   - Más adelante se mostrará la forma de establecer seguridad a esta opción de acceso.

```
Lima(config)#  line vty 0 4
Lima(config-line)# login
Lima(config-line)# password class
Lima(config-line)# ^Z
Lima# exit
```

6. **Configurando el puerto LAN (Ethernet, FastEthernet o GigaEthernet)**
   - Recordar que todo puerto está desactivado por defecto y, a su vez, se debe colocar la dirección IP. El orden de configuración no tiene relevancia.

```
Lima(config)#  interface ethernet 0
Lima(config-line)#  ip address 10.10.10.180 255.255.255.0
Lima(config-line)#  no shutdown
Lima(config-line)# ^Z
Lima# ping x.x.x.x
!!!!!
```

7. **Prueba de conexión al terminal virtual**
   - Establecer conexión Telnet desde la PC (entorno DOS).
   - Se puede realizar desde la red LAN o desde una red remota (para este caso, desde la red LAN).

```
Telnet 10.10.10.180
Password: class
Lima>enable
Lima# show running-config
```

8. **Creación de usuarios localmente**
   - Esta configuración es útil para varias alternativas de configuración, como el acceso por consola, entre otras opciones que más adelante aplicaremos.

```
Lima(config)#  Username  user01 password class
Lima(config)#  Username  user02 password class
Lima(config)#  Username  user03 password class
Lima(config)#  Username  CCNA2 password class
```

- Ejemplo de autenticación, haciendo uso de la lista local de login y password para el puerto consola. Se especifica que la autenticación se realizará utilizando la lista local de usuarios y sus contraseñas.

```
Lima(config)#  Line console 0
Lima(config-line)#  Login local
Lima(config-line)#  ^Z
Lima#  exit
--
User :
Password:
```

9. **Realizando el cifrado de contraseñas (encriptación)**
   - Se puede revisar en el archivo de configuración.

```
Lima(config)#  service password-encryption
Lima(config)# ^Z
Lima#show running-config
```

   - Anulando el comando de encriptación.

```
Lima(config)# no service password-encryption
Lima(config)# ^Z
Lima# show running-config
```

10. **Desactivando la búsqueda de dominios**

    Cuando nos equivocamos al escribir un comando, el sistema automáticamente realiza la búsqueda de dicho término como si fuera un dominio, lo cual bloquea el router para ingresar comandos.

    - Para desactivar dicha opción de búsqueda se coloca el comando **no ip domain-lookup**; se muestra un ejemplo antes de colocar el comando y después de colocarlo.

```
Router#egi
Translating “egi”...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#egi
Translating “egi”
% Unknown command or computer name, or unable to find computer address
Router#
```

11. **Creando una tabla Host**

```
Router(config)#IP HOST TFTP-SERVER 192.168.1.10
Router(config)#IP HOST RLIMA 200.1.1.1
Router(config)#EXIT
%SYS-5-CONFIG_I: Configured from console by console
Router#show host
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
     temp - temporary, perm - permanent
     NA - Not Applicable None - Not defined
Host                Port  Flags      Age Type   Address(es)
RLIMA                None  (perm, OK)  0   IP    200.1.1.1
TFTP-SERVER             None  (perm, OK)  0   IP    192.168.1.10
Router#ping RLIMA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/12/16 ms
Router#
```

12. **Copiando la configuración realizada**

- Siempre deberá guardarse la configuración del router, ya que se trabaja en la memoria RAM y podría verse interrumpida por un corte de energía.
- Para almacenar la configuración podemos emplear la NVRAM, un servidor TFTP, etc.
- La memoria RAM se indica como running-config y la memoria NVRAM se indica como startup-config, por lo que se deberá copiar la configuración activa desde la RAM.

```
Lima#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Lima#copy startup-config tftp
Address or name of remote host []? 192.168.1.3
Destination filename [Router-confg]?
.!!
[OK - 590 bytes]

590 bytes copied in 3.09 secs (0 bytes/sec)
```

13. **Eliminando la información de la NVRAM**

- Se deberá eliminar la información almacenada en la NVRAM, ya que desde ahí podría cargarse nuevamente.
- Después de ello se reinicia el router con el comando **reload**. No deberá aceptar guardar la configuración, se hace la consulta por el sistema, ya que de aceptar cargaría nuevamente la configuración, como si no se hubiese borrado.

```
Lima# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Lima# reload
Proceed with reload? [confirm]
```

14. Pruebas de acceso
    - El comando **PING** hacia todos los Hosts y routers de la topología de red.
    - Debe ser exitoso hacia cada Host o router.
    - Si el ping no es exitoso verifique el posible problema.

OBSERVACIONES Y/O COMENTARIOS

_____

_____

_____

_____

LABORATORIO Nº 3 - Diagnóstico de conexiones I

DESCRIPCIÓN

Determinar los fallos de forma efectiva es una tarea producto del conocimiento y la experiencia que se puede llegar a tener conforme se tenga un criterio ordenado para actuar de acuerdo a ciertas circunstancias. El patrón de soluciones basado en el modelo de capas es lo necesario para facilitar el entendimiento y la relación entre el hardware del router y el IOS.

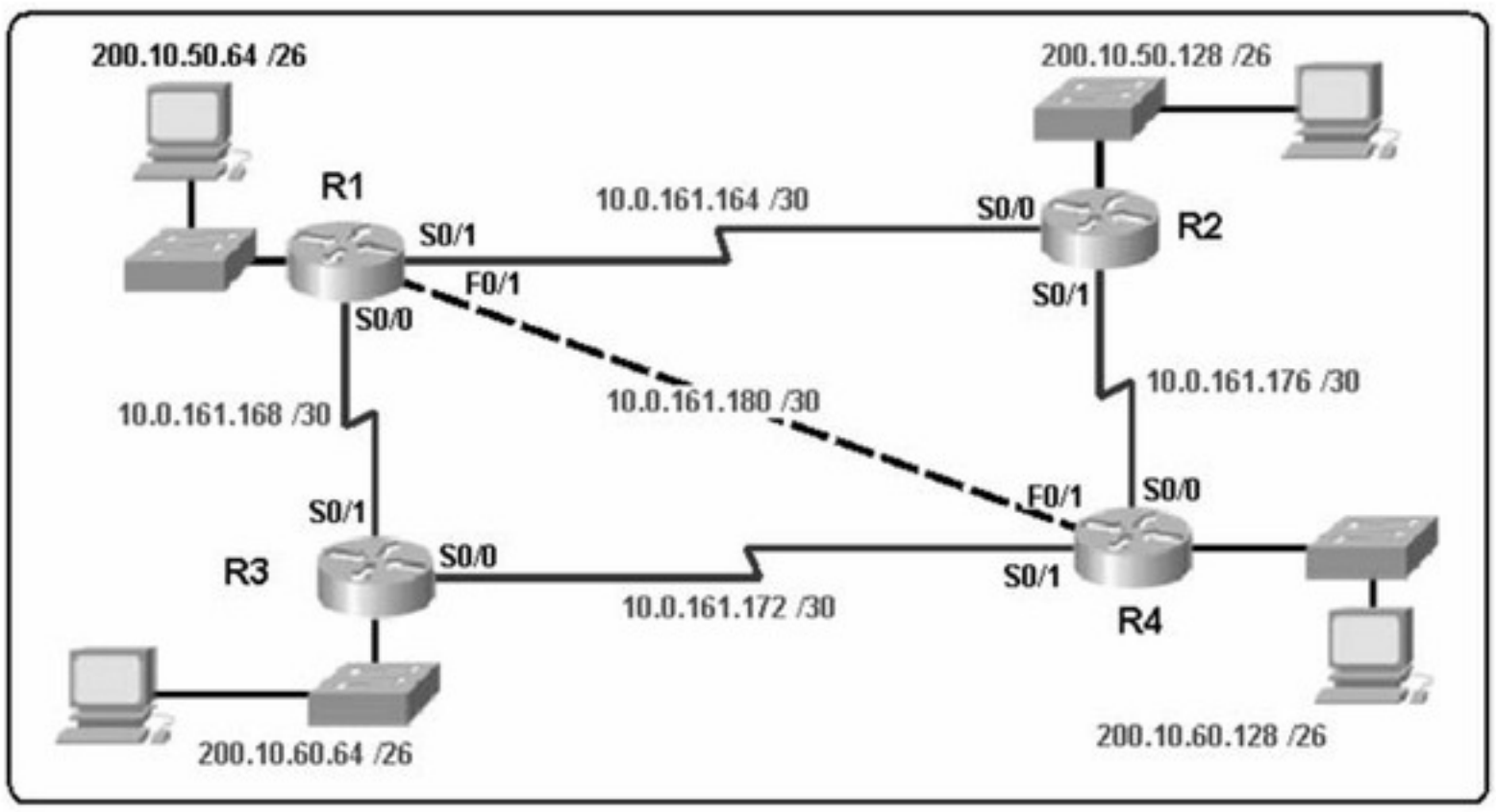
OBJETIVOS

- Determinar el uso de comandos para el diagnóstico de conexiones.
- Implementación de una topología de red en malla, con enrutamiento RIP.

DESCRIPCIÓN

La implementación es una topología en malla parcial que permite revisar los parámetros de diagnóstico con que se configura una red, así como la diferencia entre una conexión física y el enrutamiento.

Está dividida en cuatro fases que permiten ejecutar paso a paso los detalles de la configuración.



DESARROLLO

Considerando los laboratorios iniciales, se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo.

FASE I

1. Verifique el estado del router.
2. Borre la configuración del router y reinícielo.

3. Habilite la opción de captura de texto en el Hyperterminal.
4. Habilite la captura de texto de toda la ejecución de comandos.
5. Realice la configuración básica de la siguiente topología de red con ayuda del bloc de notas.
6. Verifique en su router la configuración realizada.

```
R1#sh protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 200.10.50.65/26
FastEthernet0/1 is up, line protocol is up
  Internet address is 10.0.161.182/30
Serial0/0 is up, line protocol is up
  Internet address is 10.0.161.169/30
Serial0/1 is up, line protocol is up
  Internet address is 10.0.161.166/30
```

```
R4#sh protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 200.10.60.129/26
FastEthernet0/1 is up, line protocol is up
  Internet address is 10.0.161.181/30
Serial0/0 is up, line protocol is up
  Internet address is 10.0.161.178/30
Serial0/1 is up, line protocol is up
  Internet address is 10.0.161.174/30
```

```
R3#sh run
!
!
interface FastEthernet0/0
 ip address 200.10.60.65 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 10.0.161.173 255.255.255.252
 clock rate 64000
!
interface Serial0/1
 ip address 10.0.161.170 255.255.255.252
!
!
!
```

```
R2#sh run
!
!
interface FastEthernet0/0
 ip address 200.10.60.129 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 10.0.161.165 255.255.255.252
 clock rate 64000
!
interface Serial0/1
 ip address 10.0.161.177 255.255.255.252
!
!
!
```

FASE II:

1. Realizar el diagnóstico de conexión desde el router local, empleando para ello el uso de los protocolos CDP (en la mayoría de sus opciones), ICMP y el Telnet.
   - Mediante el protocolo CDP mostrará la siguiente información (en el caso de no tener switches conectados a los routers no tendrá la información de ese equipo).

```
R1#  sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0         145          S      2950        Fas 0/1
R3           Ser 0/0         172          R      C2600       Ser 0/1
R2           Ser 0/1         144          R      C2600       Ser 0/0
R4           Fas 0/1         134          R      C2600       Fas 0/1
```

```
R2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0         156          S      2950        Fas 0/1
R1           Ser 0/0         131          R      C2600       Ser 0/1
R4           Ser 0/1         154          R      C2600       Ser 0/0
```

```
R3# sh cdp n
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          129          S       2950        Fas 0/1
R1           Ser 0/1          127          R       C2600       Ser 0/0
R4           Ser 0/0          150          R       C2600       Ser 0/1
```

- El protocolo CDP es una herramienta que podría mostrar información detallada de los vecinos, en este caso el router 4 informa en detalle de cada uno de sus vecinos, indicándose incluso la plataforma y la dirección IP del equipo vecino Cisco.

```
R4#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          164          S       2950        Fas 0/1
R3           Ser 0/1          122          R       C2600       Ser 0/0
R2           Ser 0/0          154          R       C2600       Ser 0/1
R1           Fas 0/1          121          R       C2600       Fas 0/1

R4#sh cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 139

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2
Duplex: full
---------------------------

Device ID: R3
Entry address(es):
  IP address : 10.0.161.173
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/1, Port ID (outgoing port): Serial0/0
Holdtime: 157

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
---------------------------
```

```
Device ID: R2
Entry address(es):
  IP address : 10.0.161.177
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/0, Port ID (outgoing port): Serial0/1
Holdtime: 129

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
---------------------------

Device ID: R1
Entry address(es):
  IP address : 10.0.161.182
Platform: cisco C2600, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 156

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full

R4#
```

- Con los datos del comando CDP obtenidos en R4 podemos observar lo siguiente:

		ROUTER			SWITCH
Nombre del router		R1	R2	R3	Switch
Modelo de router		C2600	C2600	C2600	2950
IOS	Software	C2600-I-M	C2600-I-M	C2600-I-M	C2950-I6Q4L2-M
	Versión	Versión 12.2(28)	Versión 12.2(28)	Versión 12.2(28)	Versión 12.1(22)EA4,
Interfaces	Interfaces	S0/1	S0/1	S0/1	F0/0
	IP	10.0.161.182	10.0.161.177	10.0.161.173	-----

- Las pruebas de Telnet y conectividad sólo podrán realizarse hacia los vecinos directamente conectados o, en todo caso, accediendo vía Telnet a un vecino y desde ahí al otro.

```
R3#ping 10.0.161.169
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.161.169, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/25/31 ms

R3#telnet 10.0.161.174
Trying 10.0.161.174 ...Open
User Access Verification
Password:
R4>ena
Password:
R4#
```

```
R2#ping 10.0.161.166

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.161.166, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/34/47 ms

R2#telnet 10.0.161.178
Trying 10.0.161.178 ...Open
User Access Verification
Password:
R4>ena
Password:
R4#
```

2. Responder las siguientes preguntas sobre la conexión.
   a. ¿Se puede comprobar con los Hosts de la LAN local? ¿Por qué?
      - Sí es posible la prueba ya que están directamente conectados.
   b. ¿Se puede comprobar con los routers vecinos? ¿Por qué?
      - Sí es posible la prueba ya que están directamente conectados.
   c. ¿Se puede comprobar con los Hosts de la redes LAN remotas? ¿Por qué?
      - No es posible la prueba ya que faltaría enrutamiento al no estar directamente conectados.
   d. ¿Se puede comprobar con los routers remotos? ¿Por qué?
      - No es posible la prueba ya que faltaría enrutamiento al no estar directamente conectados.

FASE III:

1. Habilite el enrutamiento con el protocolo RIP.

```
Router rip
Network x.x.x.x
```

2. Ejecute el comando **show IP route**.
   - Verifique que cada red no conectada directamente se encuentre listada en la tabla de enrutamiento que se presenta.

```
R1#sh ip route
Gateway of last resort is not set
    10.0.0.0/30 is subnetted, 5 subnets
C       10.0.161.164 is directly connected, Serial0/1
C       10.0.161.168 is directly connected, Serial0/0
R       10.0.161.172 [120/1] via 10.0.161.170, 00:00:06, Serial0/0
                     [120/1] via 10.0.161.181, 00:00:06, FastEthernet0/1
R       10.0.161.176 [120/1] via 10.0.161.181, 00:00:06, FastEthernet0/1
                     [120/1] via 10.0.161.165, 00:00:17, Serial0/1
C       10.0.161.180 is directly connected, FastEthernet0/1
    200.10.50.0/26 is subnetted, 1 subnets
C       200.10.50.64 is directly connected, FastEthernet0/0
R    200.10.60.0/24 [120/1] via 10.0.161.170, 00:00:06, Serial0/0
                    [120/1] via 10.0.161.181, 00:00:06, FastEthernet0/1
```

```
R4#sh ip route
Gateway of last resort is not set

    10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.164 [120/1] via 10.0.161.177, 00:00:11, Serial0/0
                     [120/1] via 10.0.161.182, 00:00:13, FastEthernet0/1
R       10.0.161.168 [120/1] via 10.0.161.173, 00:00:23, Serial0/1
                     [120/1] via 10.0.161.182, 00:00:13, FastEthernet0/1
C       10.0.161.172 is directly connected, Serial0/1
C       10.0.161.176 is directly connected, Serial0/0
C       10.0.161.180 is directly connected, FastEthernet0/1
R    200.10.50.0/24 [120/1] via 10.0.161.182, 00:00:13, FastEthernet0/1
    200.10.60.0/26 is subnetted, 1 subnets
C       200.10.60.128 is directly connected, FastEthernet0/0
```

```
R3#sh ip route

Gateway of last resort is not set

    10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.164 [120/1] via 10.0.161.169, 00:00:12, Serial0/1
C       10.0.161.168 is directly connected, Serial0/1
C       10.0.161.172 is directly connected, Serial0/0
R       10.0.161.176 [120/1] via 10.0.161.174, 00:00:24, Serial0/0
R       10.0.161.180 [120/1] via 10.0.161.174, 00:00:24, Serial0/0
                     [120/1] via 10.0.161.169, 00:00:12, Serial0/1
R    200.10.50.0/24 [120/1] via 10.0.161.169, 00:00:12, Serial0/1
    200.10.60.0/26 is subnetted, 1 subnets
C       200.10.60.64 is directly connected, FastEthernet0/0
```

```
R2#sh ip route
Gateway of last resort is not set

    10.0.0.0/30 is subnetted, 5 subnets
C       10.0.161.164 is directly connected, Serial0/0
R       10.0.161.168 [120/1] via 10.0.161.166, 00:00:08, Serial0/0
R       10.0.161.172 [120/1] via 10.0.161.178, 00:00:18, Serial0/1
C       10.0.161.176 is directly connected, Serial0/1
R       10.0.161.180 [120/1] via 10.0.161.178, 00:00:18, Serial0/1
                     [120/1] via 10.0.161.166, 00:00:08, Serial0/0
    200.10.50.0/26 is subnetted, 1 subnets
C       200.10.50.128 is directly connected, FastEthernet0/0
R    200.10.60.0/24 [120/1] via 10.0.161.178, 00:00:18, Serial0/1
```

- Si no se muestra, verifique y corrija el problema.
- En el enrutamiento RIP se habilitó sólo la versión por defecto (versión 1), que no soporta subredes, razón por la cual las tablas de enrutamiento no indican complemente todas las redes.
- Al habilitar RIP versión 2, identificamos cada una de las redes y dobles vías que algunos casos presentan.

```
Router rip
Network x.x.x.x
Version 2
No auto-summary
```

```
R1#sh ip route rip
    10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.172 [120/1] via 10.0.161.170, 00:00:10, Serial0/0
                     [120/1] via 10.0.161.181, 00:00:13, FastEthernet0/1
R       10.0.161.176 [120/1] via 10.0.161.181, 00:00:13, FastEthernet0/1
                     [120/1] via 10.0.161.165, 00:00:08, Serial0/1
    200.10.50.0/26 is subnetted, 2 subnets
R       200.10.50.128 [120/1] via 10.0.161.165, 00:00:08, Serial0/1
    200.10.60.0/26 is subnetted, 2 subnets
R       200.10.60.64 [120/1] via 10.0.161.170, 00:00:10, Serial0/0
R       200.10.60.128 [120/1] via 10.0.161.181, 00:00:13, FastEthernet0/1
```

```
R2#sh ip route rip
    10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.168 [120/1] via 10.0.161.166, 00:00:10, Serial0/0
R       10.0.161.172 [120/1] via 10.0.161.178, 00:00:27, Serial0/1
R       10.0.161.180 [120/1] via 10.0.161.178, 00:00:27, Serial0/1
                     [120/1] via 10.0.161.166, 00:00:10, Serial0/0
    200.10.50.0/26 is subnetted, 2 subnets
R       200.10.50.64 [120/1] via 10.0.161.166, 00:00:10, Serial0/0
    200.10.60.0/26 is subnetted, 2 subnets
R       200.10.60.64 [120/2] via 10.0.161.166, 00:00:10, Serial0/0
                     [120/2] via 10.0.161.178, 00:00:27, Serial0/1
R       200.10.60.128 [120/1] via 10.0.161.178, 00:00:27, Serial0/1
```

```
R3#sh ip route rip
     10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.164 [120/1] via 10.0.161.169, 00:00:02, Serial0/1
R       10.0.161.176 [120/1] via 10.0.161.174, 00:00:18, Serial0/0
R       10.0.161.180 [120/1] via 10.0.161.174, 00:00:18, Serial0/0
                     [120/1] via 10.0.161.169, 00:00:02, Serial0/1
     200.10.50.0/26 is subnetted, 2 subnets
R       200.10.50.64 [120/1] via 10.0.161.169, 00:00:02, Serial0/1
R       200.10.50.128 [120/2] via 10.0.161.169, 00:00:02, Serial0/1
                      [120/2] via 10.0.161.174, 00:00:18, Serial0/0
     200.10.60.0/26 is subnetted, 2 subnets
R       200.10.60.128 [120/1] via 10.0.161.174, 00:00:18, Serial0/0
```

```
R4#sh ip route rip
     10.0.0.0/30 is subnetted, 5 subnets
R       10.0.161.164 [120/1] via 10.0.161.177, 00:00:00, Serial0/0
                     [120/1] via 10.0.161.182, 00:00:06, FastEthernet0/1
R       10.0.161.168 [120/1] via 10.0.161.173, 00:00:20, Serial0/1
                     [120/1] via 10.0.161.182, 00:00:06, FastEthernet0/1
     200.10.50.0/26 is subnetted, 2 subnets
R       200.10.50.64 [120/1] via 10.0.161.182, 00:00:06, FastEthernet0/1
R       200.10.50.128 [120/1] via 10.0.161.177, 00:00:00, Serial0/0
     200.10.60.0/26 is subnetted, 2 subnets
R       200.10.60.64 [120/1] via 10.0.161.173, 00:00:20, Serial0/1
R4#
```

3. Realice las pruebas de conectividad necesarias con el comando **PING** hacia todos los Hosts y routers de la topología de red.
   - Debe ser exitoso hacia cada Host o router.
   - Si el ping no es exitoso verifique el posible problema.

```
R1#ping 200.10.60.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.60.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/25/31 ms

R1#ping 10.0.161.177

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.161.177, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/43/62 ms

R1#ping 200.10.60.65

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.60.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/19/32 ms
```

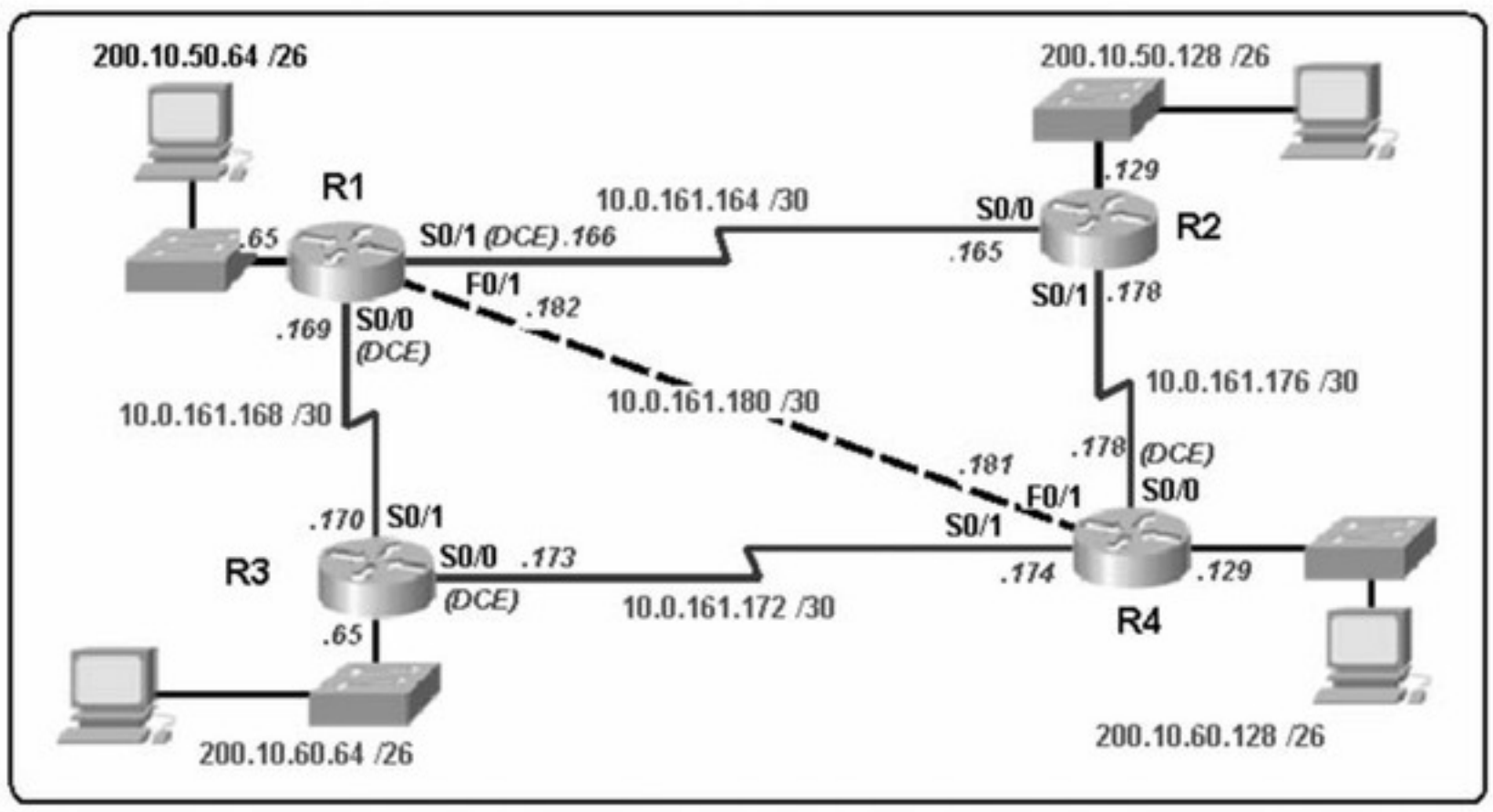
```
R2#ping 200.10.60.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.60.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 62/62/63 ms

R2#ping 200.10.50.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.10.50.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/24/31 ms

R2#ping 10.0.161.169

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.161.169, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/34/46 ms

R2#
```

4. Acceda desde su Host a cada router mediante Telnet.

```
C:\USERS\HECTOR>ipconfig
IP Address.....: 200.10.50.66
Subnet Mask.....: 255.255.255.192
Default Gateway.....: 200.10.50.65

C:\USERS\HECTOR>ping 200.10.50.65
Pinging 200.10.50.65 with 32 bytes of data:
Reply from 200.10.50.65: bytes=32 time=125ms TTL=255
Reply from 200.10.50.65: bytes=32 time=46ms TTL=255
Reply from 200.10.50.65: bytes=32 time=47ms TTL=255
Reply from 200.10.50.65: bytes=32 time=63ms TTL=255
Ping statistics for 200.10.50.65:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 46ms, Maximum = 125ms, Average = 70ms

C:\USERS\HECTOR>telnet 200.10.50.65
Trying 200.10.50.65 ...Open
User Access Verification
Password:
R1>ena
Password:
Password:
R1#exit
[Connection to 200.10.50.65 closed by foreign host]

C:\USERS\HECTOR>telnet 200.10.50.129
Trying 200.10.50.129 ...Open
User Access Verification
Password:
R2>exit
[Connection to 200.10.50.129 closed by foreign host]
```

```
C:\USERS\HECTOR>telnet 200.10.60.129
Trying 200.10.60.129 ...Open
User Access Verification
Password:
Password:
R4>
R4>exit
[Connection to 200.10.60.129 closed by foreign host]

C:\USERS\HECTOR>telnet 200.10.60.65
Trying 200.10.60.65 ...Open
User Access Verification
Password:
R3>
```

5. Realice un diagrama total de la red.
   - Direcciones IP a cada router y Host.
   - Puertos DCE y DTE.



CONCLUSIONES Y/U OBSERVACIONES

_____

_____

_____

_____

LABORATORIO Nº 4 - Diagnóstico de conexiones II

DESCRIPCIÓN

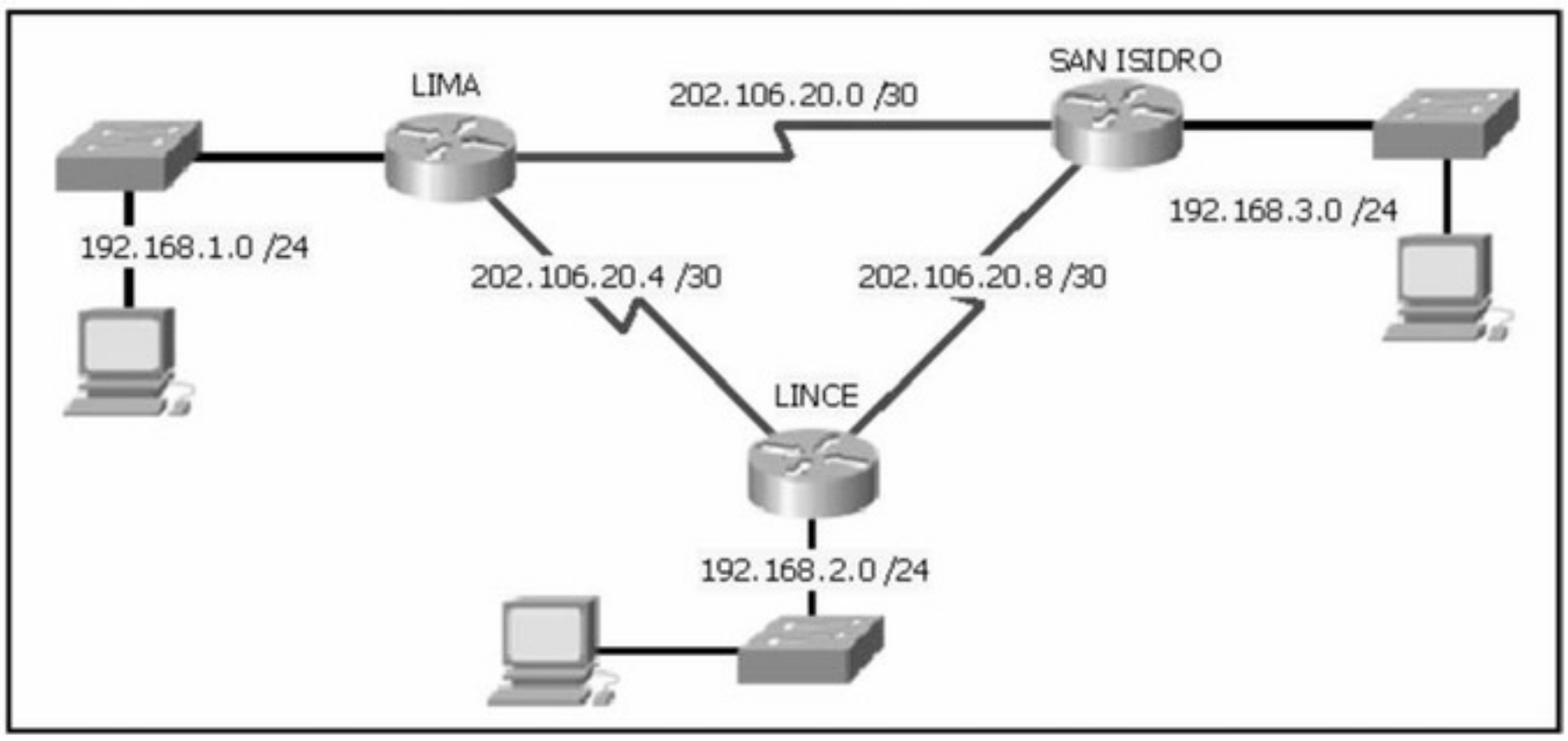
Determinar los fallos de forma efectiva es una tarea producto del conocimiento y la experiencia que se puede llegar a alcanzar conforme se tenga un criterio ordenado para actuar de acuerdo a ciertas circunstancias. El patrón de soluciones basado en el modelo de capas es lo necesario para facilitar el entendimiento y relación entre el hardware del router y el IOS.

OBJETIVOS

- Diagnóstico de conexiones en los routers.
- Análisis de fallos con la aplicación de herramientas de conectividad.

PLANTEAMIENTO

Considerando los laboratorios iniciales se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo.



- En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.
- Para realizar una configuración más adecuada verifique las interfaces seriales y Ethernet.

DESARROLLO

FASE I

1. Realice las rutinas de diagnóstico y deje listos los equipos para su configuración.
2. Realice la conexión física de los equipos en base a la topología de red.
3. Habilite la opción de captura de texto en el emulador (Hyperterminal).

FASE II

1. Realice la configuración básica de cada equipo con ayuda del bloc de notas.
2. Verifique la configuración local en cada equipo.

```
LIMA#sh runn
Building configuration...
Current configuration : 918 bytes
version 12.4
service password-encryption
!
hostname LIMA
!
enable secret 5 $1$mERr$QfS3x0SqQAcMwbwSHN8Y7.
!
ip ssh version 1
no ip domain-lookup
ip host Lince 202.106.20.6 192.168.2.1 202.106.20.9
ip host San-Isidro 202.106.20.2 192.168.3.1 202.106.20.10
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 202.106.20.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 202.106.20.5 255.255.255.252
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
banner motd ^C
ACCESO RESTRINGIDO
RED PRIVADA
^C
line con 0
 password 7 08701E1D5D4C
 logging synchronous
 login
line vty 0 4
 password 7 08701E1D5D4C53
 login
line vty 5
 password 7 08701E1D5D4C53
 login
!
end
```

3. Realice la verificación de comunicación con routers vecinos.
   - Normalmente se realiza un diagnóstico de capa 1 y capa 2, revisando la conexión física y el protocolo de línea.
   - Si ambas opciones están en **UP**, todo estará bien, pero si no, habría que revisar problemas con el cableado, los conectores, la interfaz podría estar mal colocada o desactivada, se podría necesitar el **clock rate**, etc.
   - Se presentan dos sentencias de comandos para comprobar ello.

```
LIMA#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 202.106.20.1/30
Serial0/0/1 is up, line protocol is up
  Internet address is 202.106.20.5/30
Vlan1 is administratively down, line protocol is down
```

```
LIMA#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    192.168.1.1     YES manual up                    up
FastEthernet0/1    unassigned      YES manual administratively down down
Serial0/0/0        202.106.20.1    YES manual up                    up
Serial0/0/1        202.106.20.5    YES manual up                    up
Vlan1              unassigned      YES manual administratively down down
```

   - Otra sentencia de comandos que facilita el diagnóstico es el uso del protocolo CDP.
   - Verificando la operación de capa 1 y capa 2, se nos informa de los vecinos cisco directamente conectados, junto a los detalles de cada dispositivo.
   - Se presentan dos sentencias, una con información resumida y la otra, más detallada:

```
LIMA#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme   Capability  Platform   Port ID
Sw-LIMA        Fas 0/0         138         S          2950       Fas 0/2
LINCE          Ser 0/0/1       138         R          C1841      Ser 0/0/0
SAN-ISIDRO     Ser 0/0/0       138         R          C1841      Ser 0/0/0
LIMA#
```

```
LIMA#sh cdp neighbors detail
Device ID: Sw-LIMA
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/2
Holdtime: 171
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full

---------------------------

Device ID: LINCE
Entry address(es):
  IP address : 202.106.20.6
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0
Holdtime: 171
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full

---------------------------

Device ID: SAN-ISIDRO
Entry address(es):
  IP address : 202.106.20.2
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 171
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full
```

4. Puede realizar las pruebas de conectividad si se tiene operación de capa 3.
5. En el uso de la sentencia anterior (**sh cdp neighbors detail**) se nos indicaba que se obtiene la dirección IP.
6. Teniendo la dirección IP, comprobamos si existe duplicidad para la prueba de conectividad, para acceder vía Telnet, entre otras cosas.
   - **Prueba normal de conectividad**. La prueba de conectividad es correcta con los vecinos directamente conectados; se indican cinco símbolos (!!!!!) que confirman ello pero el router no podrá acceder a la red 202.106.20.8 u otras redes, ya que necesita habilitar el enrutamiento.

```
LIMA#ping 202.106.20.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.106.20.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/16 ms

LIMA#ping 202.106.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.106.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/10/20 ms

LIMA#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/14/39 ms

LIMA#
```

- **Acceso vía TELNET**. En la prueba siguiente se muestran dos formas para acceder a los otros router, con ayuda de la tabla Host. En el primer caso se coloca el comando **Telnet Lince** y en el otro caso, directamente, el nombre del equipo registrado **San-Isidro.**

```
LIMA#telnet Lince

Trying 202.106.20.6 ...
User Access Verification
Password:
LINCE>ena
Password:
LINCE#exit
[Connection to 202.106.20.6 closed by foreign host]

LIMA#San-Isidro

Trying 202.106.20.2 ...
User Access Verification
Password:
SAN-ISIDRO>ena
Password:
SAN-ISIDRO#
SAN-ISIDRO#
```

FASE III

1. Habilite el enrutamiento dinámico con el protocolo RIP versión 2. En caso de no poder habilitar el protocolo, coloque el comando **IP routing**.
2. Visualice la tabla de enrutamiento con el comando **show IP route**.
   - Verifique que cada red no conectada directamente se encuentre listada en la tabla de enrutamiento.

```
LIMA#sh ip route
……..< resultado omitido > ……..
Gateway of last resort is not set
C   192.168.1.0/24 is directly connected, FastEthernet0/0
R   192.168.2.0/24 [120/1] via 202.106.20.6, 00:00:19, Serial0/0/1
R   192.168.3.0/24 [120/1] via 202.106.20.2, 00:00:22, Serial0/0/0
    202.106.20.0/30 is subnetted, 3 subnets
C      202.106.20.0 is directly connected, Serial0/0/0
C      202.106.20.4 is directly connected, Serial0/0/1
R      202.106.20.8 [120/1] via 202.106.20.6, 00:00:19, Serial0/0/1
                    [120/1] via 202.106.20.2, 00:00:22, Serial0/0/0
```

   - Si no se muestra, verifique y corrija el problema. Una opción recomendable es desactivar RIP y activarlo nuevamente.

3. Realice las pruebas de conectividad normal hacia todos los Hosts y routers de la topología de red.
   - Debe ser exitoso hacia cada Host o router.
   - Si el ping no es exitoso verifique el posible problema.

```
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=23ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255
Reply from 192.168.1.1: bytes=32 time=9ms TTL=255
Reply from 192.168.1.1: bytes=32 time=7ms TTL=255
Ping statistics for 192.168.1.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 7ms, Maximum = 23ms, Average = 11ms
```

   - El uso del PING EXTENDIDO permite realizar un diagnóstico desde un router hacia cualquier punto de la red empleando cualquiera de sus direcciones IP, y variar las opciones de prueba para la conectividad.
   - Por ejemplo, si el router Lima realiza un ping normal a la red LAN del router Lince, dicha prueba tendrá como IP origen al IP más cercano a ese punto, en este caso: 202.106.20.5, lo cual podríamos variar al emplear el ping extendido y usar la dirección 192.168.1.1, como se muestra en el ejemplo.
   - Este ejemplo de prueba verifica la conectividad entre ambas redes LAN.

```
LIMA#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]: 7
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 7, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!
Success rate is 100 percent (7/7), round-trip min/avg/max = 11/13/19 ms
LIMA#
```

FASE IV

Capture la siguiente información:

- Información de los vecinos.
- Configuración activa.
- Tabla de enrutamiento.

***Nota**: La captura de estos comandos está incluida en el disco adjunto al presente libro.*

OBSERVACIONES Y/O COMENTARIOS

_____

_____

_____

_____

LABORATORIO N° 5 - RIP Y LAS RUTAS DE RESPALDO

DESCRIPCIÓN

RIP versión 2 es un protocolo vector de distancia con opciones mejoradas en actualización y soporte de subredes con VLSM. Puede presentar fallos por una configuración errada, una lenta convergencia, entre otras cosas, por lo que siempre es recomendable mantener rutas de respaldo ante cualquier eventualidad.

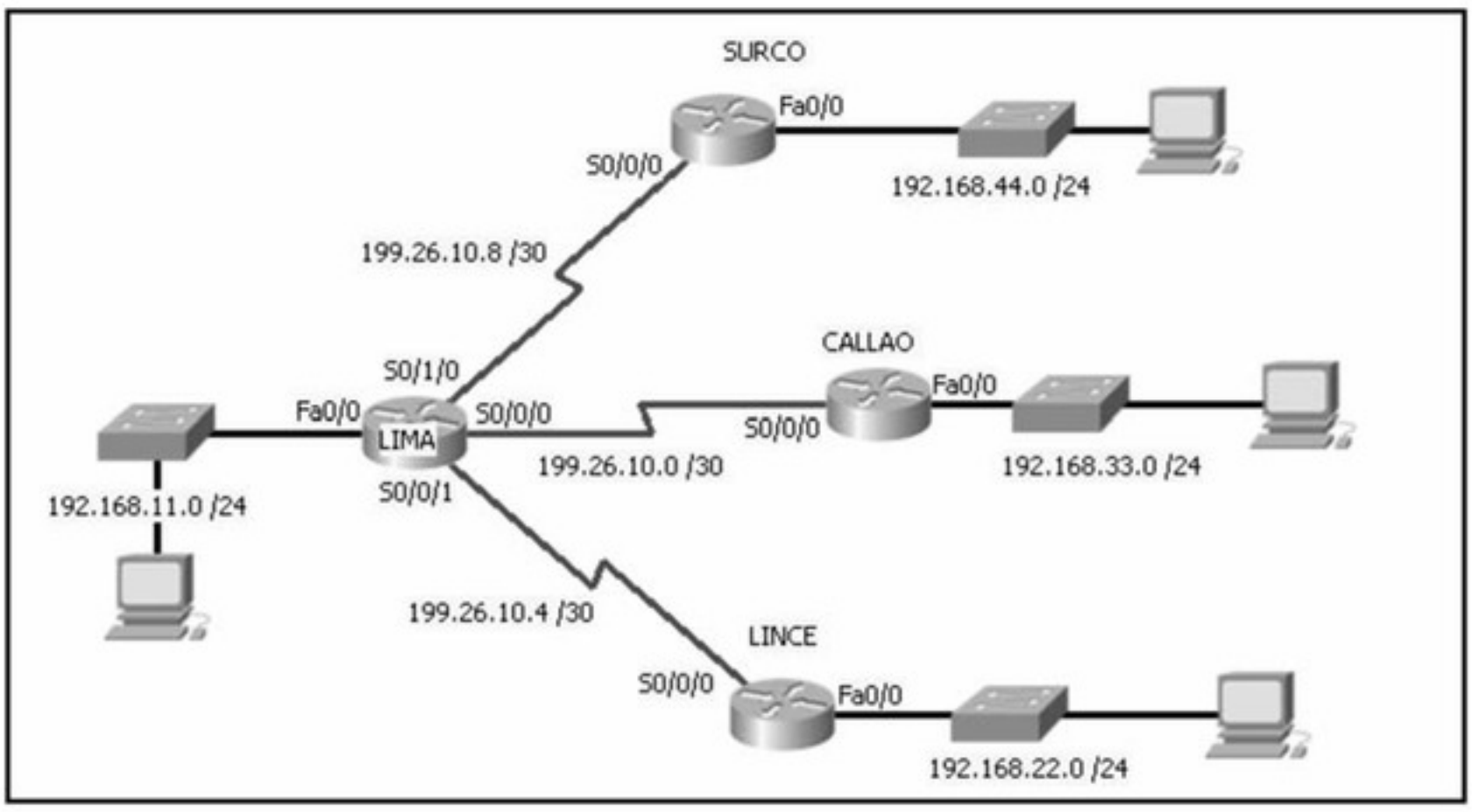
OBJETIVOS

- Analizar el comportamiento del protocolo de enrutamiento dinámico RIP.
- Comprender el uso de una ruta de respaldo (ruta backup).

PLANTEAMIENTO

Considerando que los laboratorios anteriores se complementan con el que se plantea, se efectúa una configuración para optimizar su funcionamiento.

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.



- En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.
- Para realizar una configuración más adecuada verifique las interfaces seriales y Ethernet.

DESARROLLO

FASE I

1. Realizar las conexiones y verificar la configuración de cada router.
2. Habilite la opción de captura de texto en el Hyperterminal.
3. Realice la configuración de la siguiente topología de red con ayuda un editor de texto.
4. Habilite el enrutamiento en cada router.
   a. Como se trata de una red con subredes, es más conveniente habilitar el protocolo RIP, pero en su versión 2, y deshabilitar la sumarización automática.
   b. Como se observa, en la configuración de RIP sólo se requiere mencionar la red general para el caso de las tres subredes que maneja el router.
   c. Para observar en detalle, se habilita el comando **debug ip rip** antes y luego habilitamos el enrutamiento.

```
HABILITANDO LA DEPURACIÓN PARA RIP
LIMA#debug ip rip
RIP protocol debugging is on
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

HABILITANDO EL ENRUTAMIENTO RIP V2
LIMA(config)#router rip
LIMA(config-router)#ver 2
LIMA(config-router)#no auto
LIMA(config-router)#network 192.168.11.0
LIMA(config-router)#network 199.26.10.0

Al declarase las redes, el router envía un mensaje (saludo inicial o Hello)  en multicast a la dirección
224.0.0.9, por cada interfaz incluida en dichas redes (para el caso de subredes).
RIP: sending  v2 request to 224.0.0.9 via FastEthernet0/0 (192.168.11.1)
RIP: sending  v2 request to 224.0.0.9 via Serial0/0/0 (199.26.10.1)
RIP: sending  v2 request to 224.0.0.9 via Serial0/0/1 (199.26.10.5)
RIP: sending  v2 request to 224.0.0.9 via Serial0/1/0 (199.26.10.9)

Luego se enviará una actualización por cada interfaz, indicándose las direcciones de red a las que
pertenece cada una de las otras interfaces locales.
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.11.1)
RIP: build update entries
    199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
    199.26.10.4/30 via 0.0.0.0, metric 1, tag 0
    199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (199.26.10.1)
RIP: build update entries
    192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
    199.26.10.4/30 via 0.0.0.0, metric 1, tag 0
    199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (199.26.10.5)
RIP: build update entries
    192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
    199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
    199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/1/0 (199.26.10.9)
```

```
RIP: build update entries
     192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
     199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.4/30 via 0.0.0.0, metric 1, tag 0
LIMA(config-router)#
```

Recibiendo actualización de routers vecinos vía las interfaces seriales, indicándose las redes que publican con la métrica respectiva (N° de saltos):

```
RIP: received v2 update from 199.26.10.6 on Serial0/0/1
     192.168.22.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 199.26.10.2 on Serial0/0/0
     192.168.33.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 199.26.10.10 on Serial0/1/0
     192.168.44.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 199.26.10.10 on Serial0/1/0
     192.168.44.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 199.26.10.2 on Serial0/0/0
     192.168.33.0/24 via 0.0.0.0 in 1 hops
LIMA(config-router)#
```

CONSTRUCCIÓN DE LA TABLA DE ENRUTAMIENTO

Se enviará una actualización por cada interfaz, indicándose las direcciones de red de las redes locales y remotas, ya que el router ha publicado y recibido actualizaciones.

```
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.11.1)
RIP: build update entries
     192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
     192.168.33.0/24 via 0.0.0.0, metric 2, tag 0
     192.168.44.0/24 via 0.0.0.0, metric 2, tag 0
     199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.4/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (199.26.10.1)
RIP: build update entries
     192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
     192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
     192.168.44.0/24 via 0.0.0.0, metric 2, tag 0
     199.26.10.4/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (199.26.10.5)
RIP: build update entries
     192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
     192.168.33.0/24 via 0.0.0.0, metric 2, tag 0
     192.168.44.0/24 via 0.0.0.0, metric 2, tag 0
     199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/1/0 (199.26.10.9)
RIP: build update entries
     192.168.11.0/24 via 0.0.0.0, metric 1, tag 0
     192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
     192.168.33.0/24 via 0.0.0.0, metric 2, tag 0
     199.26.10.0/30 via 0.0.0.0, metric 1, tag 0
     199.26.10.4/30 via 0.0.0.0, metric 1, tag 0

LIMA#no debug ip rip
RIP protocol debugging is off
LIMA#
```

5. Revisamos posteriormente la tabla de enrutamiento y comprobamos las redes que se han recibido.

```
LIMA#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
C   192.168.11.0/24 is directly connected, FastEthernet0/0
R   192.168.22.0/24 [120/1] via 199.26.10.6, 00:00:21, Serial0/0/1
R   192.168.33.0/24 [120/1] via 199.26.10.2, 00:00:19, Serial0/0/0
R   192.168.44.0/24 [120/1] via 199.26.10.10, 00:00:23, Serial0/1/0
    199.26.10.0/30 is subnetted, 3 subnets
C      199.26.10.0 is directly connected, Serial0/0/0
C      199.26.10.4 is directly connected, Serial0/0/1
C      199.26.10.8 is directly connected, Serial0/1/0
```

- Observe el tiempo que presenta la información de cada red actualizada vía RIP, son valores en segundos desde su ultima actualización.

```
CALLAO#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
R   192.168.11.0/24 [120/1] via 199.26.10.1, 00:00:05, Serial0/0/0
R   192.168.22.0/24 [120/2] via 199.26.10.1, 00:00:05, Serial0/0/0
C   192.168.33.0/24 is directly connected, FastEthernet0/0
R   192.168.44.0/24 [120/2] via 199.26.10.1, 00:00:05, Serial0/0/0
    199.26.10.0/30 is subnetted, 3 subnets
C      199.26.10.0 is directly connected, Serial0/0/0
R      199.26.10.4 [120/1] via 199.26.10.1, 00:00:05, Serial0/0/0
R      199.26.10.8 [120/1] via 199.26.10.1, 00:00:05, Serial0/0/0
```

```
SURCO#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
R   192.168.11.0/24 [120/1] via 199.26.10.9, 00:00:16, Serial0/0/0
R   192.168.22.0/24 [120/2] via 199.26.10.9, 00:00:16, Serial0/0/0
R   192.168.33.0/24 [120/2] via 199.26.10.9, 00:00:16, Serial0/0/0
C   192.168.44.0/24 is directly connected, FastEthernet0/0
    199.26.10.0/30 is subnetted, 3 subnets
R      199.26.10.0 [120/1] via 199.26.10.9, 00:00:16, Serial0/0/0
R      199.26.10.4 [120/1] via 199.26.10.9, 00:00:16, Serial0/0/0
C      199.26.10.8 is directly connected, Serial0/0/0
```

```
LINCE#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
R   192.168.11.0/24 [120/1] via 199.26.10.5, 00:00:28, Serial0/0/0
C   192.168.22.0/24 is directly connected, FastEthernet0/0
R   192.168.33.0/24 [120/2] via 199.26.10.5, 00:00:28, Serial0/0/0
R   192.168.44.0/24 [120/2] via 199.26.10.5, 00:00:28, Serial0/0/0
    199.26.10.0/30 is subnetted, 3 subnets
R      199.26.10.0 [120/1] via 199.26.10.5, 00:00:28, Serial0/0/0
C      199.26.10.4 is directly connected, Serial0/0/0
R      199.26.10.8 [120/1] via 199.26.10.5, 00:00:28, Serial0/0/0
```

6. Realice las pruebas de conectividad necesarias hacia todos los Hosts y routers de la topología de red. Diagnostique los posibles problemas.

FASE II ANÁLISIS DE LOS TEMPORIZADORES EN RIP

1. Configurar en el router LIMA el bloqueo de actualizaciones hacia los routers vecinos, con el comando **passive-interface default**.
   a. Luego de colocar el comando, borramos la tabla de enrutamiento con el comando **clear ip route** * y verificamos que en realidad se eliminan las redes recibidas bajo rip.
   b. Pasados unos segundos nuevamente aparecen, ya que las actualizaciones de los routers vecinos no se han cancelado.

```
LIMA(config)#router rip
LIMA(config-router)#passive-interface default
LIMA(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

LIMA#clear ip route *
LIMA#sh ip rout
…….< resultado omitido >…….

Gateway of last resort is not set
C   192.168.11.0/24 is directly connected, FastEthernet0/0
    199.26.10.0/30 is subnetted, 3 subnets
C      199.26.10.0 is directly connected, Serial0/0/0
C      199.26.10.4 is directly connected, Serial0/0/1
C      199.26.10.8 is directly connected, Serial0/1/0

LIMA#sh ip rout
…….< resultado omitido >…….

Gateway of last resort is not set
C   192.168.11.0/24 is directly connected, FastEthernet0/0
R   192.168.22.0/24 [120/1] via 199.26.10.6, 00:00:24, Serial0/0/1
R   192.168.33.0/24 [120/1] via 199.26.10.2, 00:00:23, Serial0/0/0
R   192.168.44.0/24 [120/1] via 199.26.10.10, 00:00:20, Serial0/1/0
    199.26.10.0/30 is subnetted, 3 subnets
C      199.26.10.0 is directly connected, Serial0/0/0
C      199.26.10.4 is directly connected, Serial0/0/1
C      199.26.10.8 is directly connected, Serial0/1/0
LIMA#
```

2. Verificamos en los routers vecinos el proceso de diagnóstico.
   - En el router CALLAO se muestra la configuración por defecto del protocolo RIP, respecto a los tiempos de espera, de invalidez y descarte.
   - Tenga en cuenta que dichos tiempos pueden variar en caso de que presenten problemas. Se emplea el comando **Timer Basic** seguido de los valores en tiempo.

```
CALLAO#sh ip protocols
Routing Protocol is “rip”
Sending updates every 30 seconds, next due in 25 seconds
Invalid after 180 seconds, hold down 180, flushed after 240

…….< resultado omitido >…….
```

- Se muestra además la base de datos de RIP (redes locales y redes remotas). Esta información no se modifica hasta un período de

```
LINCE#sh ip rip database
192.168.11.0/24
    [1] via 199.26.10.5, 00:00:26, Serial0/0/0
192.168.22.0/24    directly connected, FastEthernet0/0
192.168.33.0/24
    [2] via 199.26.10.5, 00:00:26, Serial0/0/0
192.168.44.0/24
    [2] via 199.26.10.5, 00:00:26, Serial0/0/0
199.26.10.0/30
    [1] via 199.26.10.5, 00:00:26, Serial0/0/0
199.26.10.4/30    directly connected, Serial0/0/0
199.26.10.8/30
    [1] via 199.26.10.5, 00:00:26, Serial0/0/0
```

- El router CALLAO, como no recibe actualizaciones del router LIMA por un período mayor a los 30 segundos, pone en espera a las redes recibidas mediante RIP por 180 segundos, a la vez que se toma en cuenta el tiempo de invalidez, que también es de 180 segundos.

```
CALLAO#sh ip route
……..< resultado omitido >…….

Gateway of last resort is not set
R    192.168.11.0/24 [120/1] via 199.26.10.1, 00:01:17, Serial0/0/0
R    192.168.22.0/24 [120/2] via 199.26.10.1, 00:01:17, Serial0/0/0
C    192.168.33.0/24 is directly connected, FastEthernet0/0
R    192.168.44.0/24 [120/2] via 199.26.10.1, 00:01:17, Serial0/0/0
     199.26.10.0/30 is subnetted, 3 subnets
C       199.26.10.0 is directly connected, Serial0/0/0
R       199.26.10.4 [120/1] via 199.26.10.1, 00:01:17, Serial0/0/0
R       199.26.10.8 [120/1] via 199.26.10.1, 00:01:17, Serial0/0/0
```

- Después de pasar el tiempo de espera e invalidez (180 segundos) y no recibir actualizaciones del router LIMA, se declara el período de descarte (240 segundos) y se desactivan las redes recibidas (**possibly down**).

```
CALLAO#sh ip route
……..< resultado omitido >…….

Gateway of last resort is not set
R    192.168.11.0/24 is possibly down, routing via 199.26.10.1, Serial0/0/0
R    192.168.22.0/24 is possibly down, routing via 199.26.10.1, Serial0/0/0
C    192.168.33.0/24 is directly connected, FastEthernet0/0
R    192.168.44.0/24 is possibly down, routing via 199.26.10.1, Serial0/0/0
     199.26.10.0/30 is subnetted, 3 subnets
C       199.26.10.0 is directly connected, Serial0/0/0
R       199.26.10.4 is possibly down, routing via 199.26.10.1, Serial0/0/0
R       199.26.10.8 is possibly down, routing via 199.26.10.1, Serial0/0/0
```

- La base de datos de RIP también indican que las redes recibidas están posiblemente desactivadas (**possibly down**).

```
CALLAO#sh ip rip database
192.168.11.0/24
    [16] is possibly down, via 199.26.10.5, 00:03:42, Serial0/0/0
192.168.22.0/24    directly connected, FastEthernet0/0
192.168.33.0/24
    [16] is possibly down, via 199.26.10.5, 00:03:42, Serial0/0/0
192.168.44.0/24
    [16] is possibly down, via 199.26.10.5, 00:03:42, Serial0/0/0
199.26.10.0/30
    [16] is possibly down, via 199.26.10.5, 00:03:42, Serial0/0/0
199.26.10.4/30    directly connected, Serial0/0/0
199.26.10.8/30
    [16] is possibly down, via 199.26.10.5, 00:03:42, Serial0/0/0
```

- Las características de operación del protocolo RIP indican que se siguen enviando actualizaciones por parte del router CALLAO (**Sending updates every 30 seconds, next due in 22 seconds**), así como la información de la última actualización recibida, donde las fuentes de información de enrutamiento indican que para el caso es de 06:59 minutos (**Routing Information Sources**).

```
CALLAO#sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 22 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0    2     2
  Serial0/0/0        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
    192.168.22.0
    199.26.10.0
Passive Interface(s):
Routing Information Sources:
    Gateway         Distance      Last Update
    199.26.10.5          120      00:06:59
Distance: (default is 120)
```

- El router LIMA no se ve afectado en lo concerniente a la recepción de actualizaciones RIP, ya que los routers vecinos siguen emitiendo actualizaciones.

```
LIMA#sh ip route
……<resultado omitido>……
Gateway of last resort is not set
C   192.168.11.0/24 is directly connected, FastEthernet0/0
R   192.168.22.0/24 [120/1] via 199.26.10.6, 00:00:21, Serial0/0/1
R   192.168.33.0/24 [120/1] via 199.26.10.2, 00:00:19, Serial0/0/0
R   192.168.44.0/24 [120/1] via 199.26.10.10, 00:00:23, Serial0/1/0
    199.26.10.0/30 is subnetted, 3 subnets
C      199.26.10.0 is directly connected, Serial0/0/0
C      199.26.10.4 is directly connected, Serial0/0/1
C      199.26.10.8 is directly connected, Serial0/1/0
```

- Terminado el período de descarte viene el período de invalidez (180 segundos), donde las redes son retiradas de la tabla de enrutamiento pero no se eliminan del todo.

```
CALLAO#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.33.0/24 is directly connected, FastEthernet0/0
     199.26.10.0/30 is subnetted, 1 subnets
C       199.26.10.0 is directly connected, Serial0/0/0
```

- La base de datos de RIP indica que ya no hay información de redes remotas.

```
CALLAO#sh ip rip database
192.168.33.0/24    directly connected, FastEthernet0/0
199.26.10.0/30    directly connected, Serial0/0/0
```

- Las características de operación del protocolo RIP ya no indican datos de las fuentes de información de enrutamiento (**Routing Information Sources**).

```
CALLAO#sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0    2     2
  Serial0/0/0        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     192.168.33.0
     199.26.10.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
Distance: (default is 120)
```

FASE III RUTAS ESTÁTICAS COMO RESPALDO

1. **RUTA POR DEFECTO**:
   - Para permitir que los routers sigan comunicándose podemos habilitar una ruta por defecto en cada router final, considerando que el router LIMA sigue recibiendo las redes publicadas bajo RIP.
   - Esta ruta podría haberse configurado desde antes del problema y estaría considerada como una ruta de respaldo (ruta backup).

- No habría generado conflicto con RIP, ya que el sistema consultaría primero a las redes de RIP y al final, a la ruta por defecto.

```
CALLAO#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
C    192.168.33.0/24 is directly connected, FastEthernet0/0
     199.26.10.0/30 is subnetted, 1 subnets
C       199.26.10.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

- Las rutas por defecto son empleadas en routers de borde para alcanzar un conjunto de redes, como en el caso de Internet, simplificando la tabla de enrutamiento.
- Una ruta por defecto no puede configurarse en ambos extremos de un enlace ya que podrían generarse bucles.

2. RUTA ESTÁTICA

- Una alternativa adicional es emplear rutas estáticas en cada router de extremo, con la diferencia de que se tendría que crear una ruta para cada red de la topología.
- Si las rutas estáticas estuvieran activas a la vez que RIP, el sistema emplearía las rutas estáticas por tener una distancia administrativa menor.

```
LINCE#sh ip route
……..< resultado omitido >…….
Gateway of last resort is not set
S    192.168.11.0/24 is directly connected, Serial0/0/0
C    192.168.22.0/24 is directly connected, FastEthernet0/0
S    192.168.33.0/24 is directly connected, Serial0/0/0
S    192.168.44.0/24 is directly connected, Serial0/0/0
     199.26.10.0/30 is subnetted, 1 subnets
C       199.26.10.4 is directly connected, Serial0/0/0
```

- Varíe la distancia administrativa de las rutas estáticas para evitar que el sistema las emplee antes que RIP (ruta backup).
- En el ejemplo se indica la distancia administrativa de las rutas por defecto que se asignaron al router LINCE.

```
LINCE#sh ip route 192.168.11.0
Routing entry for 192.168.11.0/24
Known via "static", distance 180, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1
LINCE#sh ip route 192.168.33.0
Routing entry for 192.168.33.0/24
Known via "static", distance 180, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1
LINCE#sh ip route 192.168.44.0
Routing entry for 192.168.44.0/24
Known via "static", distance 180, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1
LINCE#
```

3. Después de la configuración de las rutas estáticas y por defecto, observamos que el sistema se restablece y nuevamente se publican las actualizaciones de RIP.
4. Las tablas de enrutamiento de los routers que fueron configurados se muestran a continuación:
   - El router CALLAO fue configurado con ruta por defecto y se muestra al final de la tabla de enrutamiento.

```
CALLAO#sh ip rou
……..< resultado omitido >…….
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
R    192.168.11.0/24 [120/1] via 199.26.10.1, 00:00:13, Serial0/0/0
C    192.168.33.0/24 is directly connected, FastEthernet0/0
R    192.168.44.0/24 [120/2] via 199.26.10.1, 00:00:13, Serial0/0/0
     199.26.10.0/30 is subnetted, 3 subnets
C       199.26.10.0 is directly connected, Serial0/0/0
R       199.26.10.4 [120/1] via 199.26.10.1, 00:00:13, Serial0/0/0
R       199.26.10.8 [120/1] via 199.26.10.1, 00:00:13, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
CALLAO#
```

```
SURCO#sh ip rout
……..< resultado omitido >…….
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
R    192.168.11.0/24 [120/1] via 199.26.10.9, 00:00:01, Serial0/0/0
R    192.168.33.0/24 [120/2] via 199.26.10.9, 00:00:01, Serial0/0/0
C    192.168.44.0/24 is directly connected, FastEthernet0/0
     199.26.10.0/30 is subnetted, 3 subnets
R       199.26.10.0 [120/1] via 199.26.10.9, 00:00:01, Serial0/0/0
R       199.26.10.4 [120/1] via 199.26.10.9, 00:00:01, Serial0/0/0
C       199.26.10.8 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

   - El router LINCE fue configurado con rutas estáticas, variando sus distancias administrativas. No aparecen las rutas estáticas.

```
LINCE#sh ip rout
……..< resultado omitido >…….
Gateway of last resort is not set
R    192.168.11.0/24 [120/1] via 199.26.10.5, 00:00:06, Serial0/0/0
C    192.168.22.0/24 is directly connected, FastEthernet0/0
R    192.168.33.0/24 [120/2] via 199.26.10.5, 00:00:06, Serial0/0/0
R    192.168.44.0/24 [120/2] via 199.26.10.5, 00:00:06, Serial0/0/0
     199.26.10.0/30 is subnetted, 3 subnets
R       199.26.10.0 [120/1] via 199.26.10.5, 00:00:06, Serial0/0/0
C       199.26.10.4 is directly connected, Serial0/0/0
R       199.26.10.8 [120/1] via 199.26.10.5, 00:00:06, Serial0/0/0
```

FASE IV

1. Realice las pruebas de conectividad necesarias hacia todos los Hosts y routers de la topología de red.
2. Diagnostique cualquier problema que se presente.

FASE V

1. Capture los datos de configuración de cada router.
   - Configuración activa.
   - Tabla de enrutamiento.

OBSERVACIONES Y/O COMENTARIOS

LABORATORIO N° 6 - Redistribución de rutas estáticas en RIP

DESCRIPCIÓN

El empleo del enrutamiento dinámico y estático en una red requiere de un proceso conocido como redistribución, el cual facilita la integración de las redes dentro del enrutamiento dinámico y la convergencia de una topología.

Dependiendo del escenario que se plantee puede resultar necesaria una ruta por defecto, una ruta estática o ambas, considerando la ubicación de cada equipo.

OBJETIVOS

- Redistribución de rutas estáticas y por defecto en las actualizaciones RIP.
- Analizar la aplicación de las rutas por defecto.

PLANTEAMIENTO

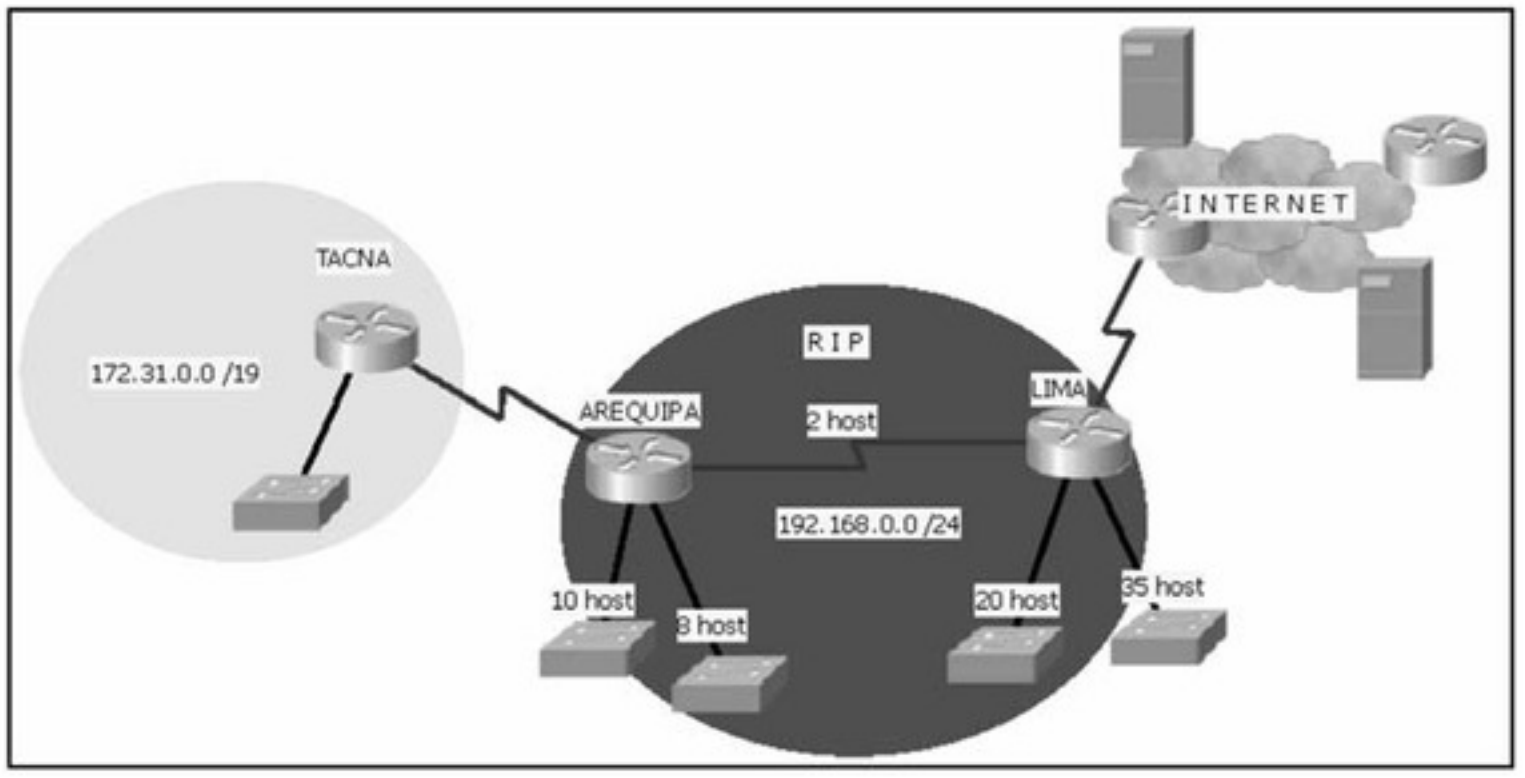
Considerando que los laboratorios anteriores se complementan con el que se plantea, se efectúa una configuración para optimizar su funcionamiento.

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

CASO 1:

El presente laboratorio tiene como propósito utilizar la combinación del protocolo RIP, en conjunto con la ruta por defecto y las rutas estáticas.

Se cita como caso el hecho de que la red hacia el router Tacna es una sucursal, o un socio comercial que en un primer momento no se encuentra y luego se añade.



- En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.
- Para realizar una configuración más adecuada verifique las interfaces seriales y Ethernet.

1. Realice las conexiones y verifique la configuración de cada router.
2. Habilite la opción de captura de texto en el Hyperterminal.
3. Realice la configuración de la siguiente topología de red con ayuda un editor de texto.
4. Solucionado el tema de direccionamiento por VLSM se tendrá la siguiente solución:

	INTERFAZ	DIRECCIÓN IP
LIMA	Fa0/0	192.168.0.1 /26
	Fa0/1	192.168.0.65 /27
	S0/0/0	192.168.0.130 /30
	S0/0/1	202.1.1.1 /30
AREQUIPA	Fa0/0	192.168.0.97 /28
	Fa0/1	192.168.0.113 /28
	S0/0/0	192.168.0.129 /30
	S0/0/1	200.23..0.1 /30
TACNA	Fa0/0	172.31.0.1 /19
	S0/0/0	200.23.0.2 /30
ISP	S0/0/0	202.1.1.2 /30
	L 0	200.0.0.1 /24
	L 1	203.3.3.1 /24

5. Habilite el enrutamiento en cada router según lo siguiente:
   - El router Lima habilitará el RIP y la ruta por defecto hacia el ISP.
   - El router Arequipa tendrá que habilitarse el RIP y una ruta estática para llegar a la red del router Tacna.
   - El router Tacna manejará una ruta estática para llegar a la red de Arequipa y Lima, o una ruta por defecto si necesita llegar a Internet.
   - El router ISP deberá manejar una ruta estática hacia la red de Arequipa y Lima, además de una ruta estática si se le quiere permitir a la red del router Tacna llegar a Internet.

6. DESARROLLO:
   1. En los routers Lima y Arequipa se habilita el protocolo RIP y se muestra la tabla de enrutamiento en ambos equipos como sigue:

```
AREQUIPA#SH IP ROUTE
……..<resultado omitido>……
Gateway of last resort is not set
      192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
R     192.168.0.0/26 [120/1] via 192.168.0.130, 00:00:00, Serial0/0/0
R     192.168.0.64/27 [120/1] via 192.168.0.130, 00:00:00, Serial0/0/0
C     192.168.0.96/28 is directly connected, FastEthernet0/0
C     192.168.0.112/28 is directly connected, FastEthernet0/1
C     192.168.0.128/30 is directly connected, Serial0/0/0
```

```
LIMA#SH IP ROUTE
……..<resultado omitido>……
Gateway of last resort is not set
      192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
C     192.168.0.0/26 is directly connected, FastEthernet0/0
C     192.168.0.64/27 is directly connected, FastEthernet0/1
R     192.168.0.96/28 [120/1] via 192.168.0.129, 00:00:09, Serial0/0/0
R     192.168.0.112/28 [120/1] via 192.168.0.129, 00:00:09, Serial0/0/0
C     192.168.0.128/30 is directly connected, Serial0/0/0
```

2. Habilitamos el enrutamiento para Internet en el router Lima mediante una ruta por defecto:

```
LIMA(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1
```

- El router ISP deberá tener una ruta estática que permita ingresar a los paquetes desde Internet; asimismo, habilitamos dos interfaces loopback en el router ISP que permitan representar servidores de Internet.

```
ISP(config)#ip route 192.168.0.0 255.255.255.0 s0/0/0
ISP(config)#int loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip add 200.0.0.1 255.255.255.0
ISP(config-if)#int loopback 1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ISP(config-if)#ip add 203.3.3.1 255.255.255.0
ISP(config-if)#^Z
```

- Revisamos la tabla de enrutamiento del router Lima, comprobando que la ruta por defecto está integrada.

```
LIMA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
C      192.168.0.0/26 is directly connected, FastEthernet0/0
C      192.168.0.64/27 is directly connected, FastEthernet0/1
R      192.168.0.96/28 [120/1] via 192.168.0.129, 00:00:22, Serial0/0/0
R      192.168.0.112/28 [120/1] via 192.168.0.129, 00:00:22, Serial0/0/0
C      192.168.0.128/30 is directly connected, Serial0/0/0
    202.2.2.0/30 is subnetted, 1 subnets
C      202.2.2.0 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

- Realizamos pruebas de conectividad hacia las interfaces Loopback creadas en el router ISP. Primero se deben realizar las pruebas con un ping normal desde el router.

- Realizar un ping extendido empleando las direcciones IP de las interfaces FastEthernet como IP de origen. Se indicará que todo Host de las redes Lan de Lima podrán llegar a Internet.

```
LIMA#ping 200.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
LIMA#ping 203.3.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/5 ms
LIMA#ping
Protocol [ip]:
Target IP address: 200.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/11 ms

LIMA#ping
Protocol [ip]:
Target IP address: 203.3.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.0.65
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.3.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.65
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
```

- El router Arequipa aún no puede alcanzar Internet, ya que su tabla de enrutamiento no conoce ruta alguna.

```
AREQUIPA#ping 203.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.3.3.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
AREQUIPA#ping 200.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

AREQUIPA#SH IP ROUTE
……..<resultado omitido>……
Gateway of last resort is not set
    192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
R       192.168.0.0/26 [120/1] via 192.168.0.130, 00:00:09, Serial0/0/0
R       192.168.0.64/27 [120/1] via 192.168.0.130, 00:00:09, Serial0/0/0
C       192.168.0.96/28 is directly connected, FastEthernet0/0
C       192.168.0.112/28 is directly connected, FastEthernet0/1
C       192.168.0.128/30 is directly connected, Serial0/0/0
```

- Luego tendremos que redistribuir la ruta por defecto dentro de la actualización RIP para que el router Arequipa pueda llegar a Internet.

```
LIMA(config)#router rip
LIMA(config-router)#default-information originate
```

- Verificamos luego el router Arequipa.

```
AREQUIPA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 192.168.0.130 to network 0.0.0.0
    192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
R       192.168.0.0/26 [120/1] via 192.168.0.130, 00:00:01, Serial0/0/0
R       192.168.0.64/27 [120/1] via 192.168.0.130, 00:00:01, Serial0/0/0
C       192.168.0.96/28 is directly connected, FastEthernet0/0
C       192.168.0.112/28 is directly connected, FastEthernet0/1
C       192.168.0.128/30 is directly connected, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 192.168.0.130, 00:00:01, Serial0/0/0

AREQUIPA#ping 200.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/7/9 ms

AREQUIPA#ping 203.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.3.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/13 ms
```

3. Finalmente configuramos en el router Arequipa una ruta estática hacia la red de Tacna, para luego configurar en Tacna una ruta estática para llegar a la red de Arequipa y Lima, o una ruta por defecto si necesita llegar a Internet.

```
AREQUIPA(config-if)#ip address 200.23.0.1 255.255.255.252

AREQUIPA#SH IP ROUTE
……..<resultado omitido>……
Gateway of last resort is 192.168.0.130 to network 0.0.0.0
    172.31.0.0/19 is subnetted, 1 subnets
S      172.31.0.0 is directly connected, Serial0/0/1
    192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
R      192.168.0.0/26 [120/1] via 192.168.0.130, 00:00:17, Serial0/0/0
R      192.168.0.64/27 [120/1] via 192.168.0.130, 00:00:17, Serial0/0/0
C      192.168.0.96/28 is directly connected, FastEthernet0/0
C      192.168.0.112/28 is directly connected, FastEthernet0/1
C      192.168.0.128/30 is directly connected, Serial0/0/0
    200.23.0.0/30 is subnetted, 1 subnets
C      200.23.0.0 is directly connected, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 192.168.0.130, 00:00:17, Serial0/0/0
```

```
TACNA(config)#ip route 192.168.0.0 255.255.255.0 s0/0/0
```

- Verificamos la conectividad y comprobamos que el router Tacna no puede llegar hasta el router Lima, sólo a las Lan de Arequipa.

```
TACNA#PING 192.168.0.97
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.97, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/6 ms
TACNA#PING 192.168.0.113
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.113, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
TACNA#PING 192.168.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

- Se necesita habilitar una redistribución de la ruta estática dentro del RIP y así se publicará ésta, para que el router Lima pueda conocer la red de Tacna.

```
AREQUIPA(config)#router rip
AREQUIPA(config-router)#redistribute static
```

```
LIMA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.31.0.0/19 is subnetted, 1 subnets
R      172.31.0.0 [120/1] via 192.168.0.129, 00:00:04, Serial0/0/0
    192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
C      192.168.0.0/26 is directly connected, FastEthernet0/0
C      192.168.0.64/27 is directly connected, FastEthernet0/1
R      192.168.0.96/28 [120/1] via 192.168.0.129, 00:00:04, Serial0/0/0
R      192.168.0.112/28 [120/1] via 192.168.0.129, 00:00:04, Serial0/0/0
C      192.168.0.128/30 is directly connected, Serial0/0/0
    202.2.2.0/30 is subnetted, 1 subnets
C      202.2.2.0 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

4. Si el router de Tacna necesita llegar a Internet, deberá añadir o reemplazar su ruta estática por una ruta por defecto; asimismo, el router ISP deberá manejar una ruta estática hacia la red de Tacna.

```
TACNA(config)#no ip route 192.168.0.0 255.255.255.0 s0/0/0
TACNA(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

```
ISP(config)#ip route 172.23.0.0 255.255.224.0 s0/0/0
```

```
TACNA#ping 200.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms

TACNA#ping 203.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.3.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/5 ms
```

OBSERVACIONES Y/O COMENTARIOS

_____

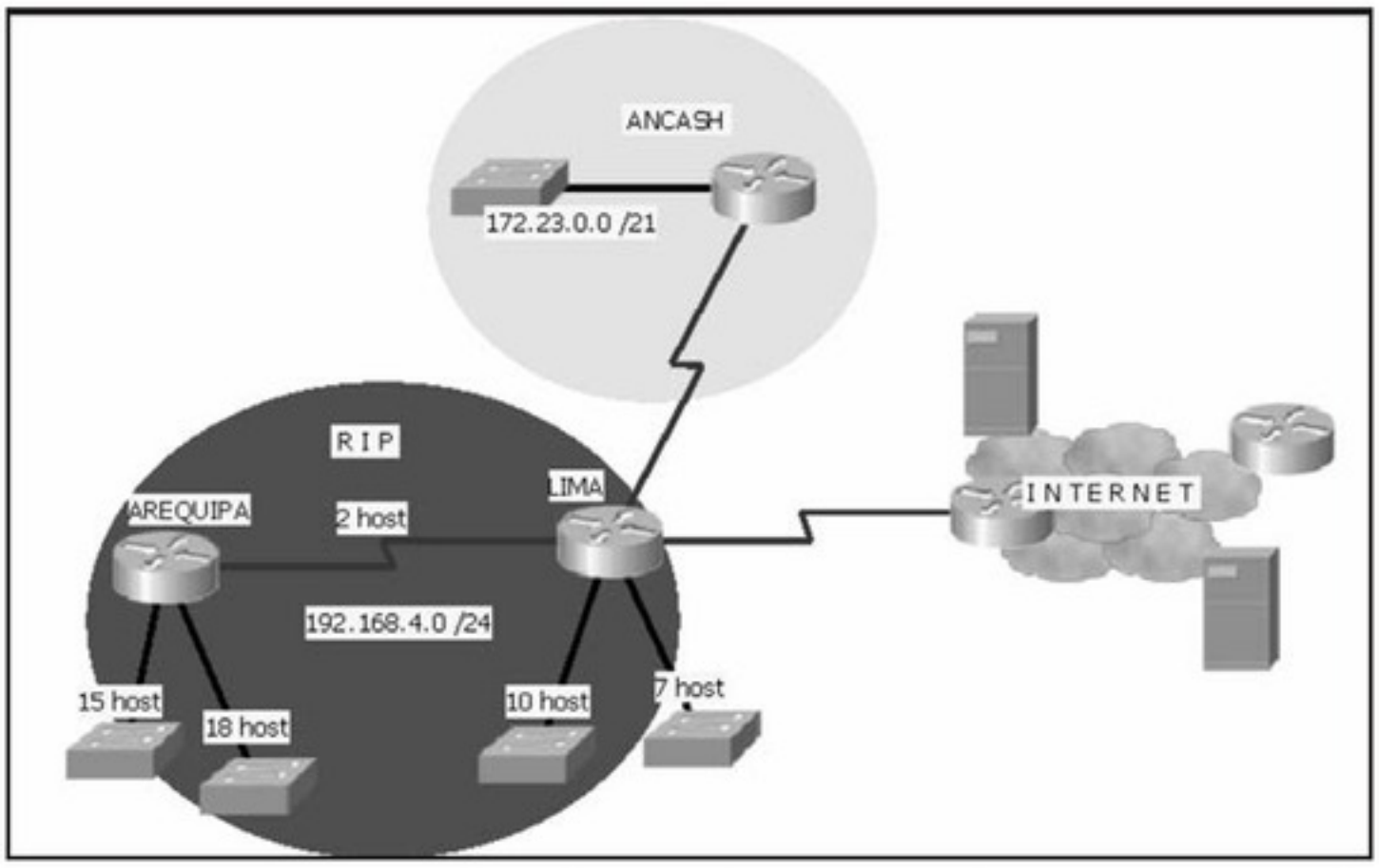
_____

_____

_____

CASO 2:

Teniendo en cuenta los problemas y el análisis del caso anterior, se plantea un caso parecido, donde podremos agregar en diferentes ubicaciones la ruta estática y la ruta por defecto.



- En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.
- Para realizar una configuración más adecuada verifique las interfaces seriales y Ethernet.

I. Realice las conexiones y verifique la configuración de cada router.

II. Habilite la opción de captura de texto en el Hyperterminal.

III. Realice la configuración de la siguiente topología de red con ayuda un editor de texto.

IV. Solucionado el tema de direccionamiento por VLSM se tendrá la siguiente solución:

	INTERFAZ	DIRECCIÓN IP
LIMA	Fa0/0	192.168.4.65 /28
	Fa0/1	192.168.4.81 /28
	S0/0/0	192.168.4.130 /30
	S0/0/1	202.2.2.1 /30
	S0/1/0	201.1.1.1 /30
AREQUIPA	Fa0/0	192.168.4.1 /27
	Fa0/1	192.168.4.33 /27
	S0/0/0	192.168.4.129 /30
ANCASH	Fa0/0	172.23.0.1 /21
	S0/0/0	201.1.1.2 /30
ISP	S0/0/0	202.2.2.2 /30

V. Habilite el enrutamiento en cada router según lo siguiente:

- El router Lima habilitará el RIP y la ruta por defecto hacia el ISP, además de una ruta estática hacia la red del router Ancash.
- El router Arequipa tendrá solamente que habilitar el RIP.
- El router Ancash manejará una ruta estática para llegar a la red de Arequipa y Lima, o una ruta por defecto si necesita llegar a Internet.
- El router ISP deberá manejar una ruta estática hacia la red de Arequipa y Lima, además de una ruta estática si se quiere permitir a la red del router Ancash llegar a Internet.

VI. DESARROLLO:

1. El router Lima centraliza la mayor configuración de la topología, por lo que deberá desarrollarse más detenidamente.
   - Habilitar el RIP para su comunicación con el router Arequipa.
   - Establecer una ruta por defecto hacia el ISP, además de redistribuir la ruta hacia Arequipa vía RIP.
   - Establecer una ruta estática hacia la red del router Ancash, además de redistribuir la ruta hacia Arequipa vía RIP.

```
LIMA(config)#router rip
LIMA(config-router)# version 2
LIMA(config-router)# no auto-summary
LIMA(config-router)# network 192.168.4.0
LIMA(config-router)#exit

LIMA(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/1
LIMA(config)#router rip
LIMA(config-router)# default-information originate
LIMA(config-router)#exit

LIMA(config)#ip route 172.23.0.0 255.255.248.0 Serial0/1/0 LIMA(config)#router rip
LIMA(config-router)# redistribute static
```

   - En realidad esta última opción no es necesaria ya que el router LIMA ha enviado una redistribución de la ruta por defecto que sumariza todas las redes, de tal forma que el router ya no envía la redistribución de la ruta estática.
   - Habilitamos la depuración para comprobar dichas actualizaciones y se verifica la mención anterior.

```
RIP protocol debugging is on
LIMA#RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.4.65)
RIP: build update entries
    0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
    192.168.4.0/27 via 0.0.0.0, metric 2, tag 0
    192.168.4.32/27 via 0.0.0.0, metric 2, tag 0
    192.168.4.80/28 via 0.0.0.0, metric 1, tag 0
    192.168.4.128/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via FastEthernet0/1 (192.168.4.81)
RIP: build update entries
    0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
    192.168.4.0/27 via 0.0.0.0, metric 2, tag 0
    192.168.4.32/27 via 0.0.0.0, metric 2, tag 0
    192.168.4.64/28 via 0.0.0.0, metric 1, tag 0
    192.168.4.128/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (192.168.4.130)
RIP: build update entries
    0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
    192.168.4.64/28 via 0.0.0.0, metric 1, tag 0
    192.168.4.80/28 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 192.168.4.129 on Serial0/0/0
    192.168.4.0/27 via 0.0.0.0 in 1 hops
    192.168.4.32/27 via 0.0.0.0 in 1 hops
undebug all
All possible debugging has been turned off
LIMA#
```

- La depuración demuestra que el router Lima está actualizando a través de todas sus interfaces, sin embargo, sólo es necesario mantener activa la interfaz serial 0/0/0.
- Para este caso colocamos el comando **passive-interface** para bloquear dichas actualizaciones.

```
LIMA(config)#router rip
LIMA(config-router)#passive-interface s0/0/1
LIMA(config-router)#passive-interface s0/1/0
LIMA(config-router)#passive-interface f0/0
LIMA(config-router)#passive-interface f0/1
LIMA(config-router)#
```

- Verificamos la depuración.

```
LIMA#debug ip rip
RIP protocol debugging is on
LIMA#RIP: received v2 update from 192.168.4.129 on Serial0/0/0
     192.168.4.0/27 via 0.0.0.0 in 1 hops
     192.168.4.32/27 via 0.0.0.0 in 1 hops
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (192.168.4.130)
RIP: build update entries
     0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
     192.168.4.64/28 via 0.0.0.0, metric 1, tag 0
     192.168.4.80/28 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 192.168.4.129 on Serial0/0/0
```

2. El router Arequipa tendrá solamente que habilitar RIP.
3. El router ANCASH manejará una ruta estática para llegar a la red de Arequipa y Lima, o una ruta por defecto si necesita llegar a Internet.
4. El router ISP deberá manejar una ruta estática hacia la red de Arequipa y Lima, además de una ruta estática si se quiere permitir a la red del router Ancash llegar a Internet.

```
ISP#sh ip route
……..<resultado omitido>……
Gateway of last resort is not set
    172.23.0.0/21 is subnetted, 1 subnets
S      172.23.0.0 is directly connected, Serial0/0/0
S    192.168.4.0/24 is directly connected, Serial0/0/0
    202.2.2.0/30 is subnetted, 1 subnets
C       202.2.2.0 is directly connected, Serial0/0/0
C    220.1.1.0/24 is directly connected, Loopback0
C    220.2.2.0/24 is directly connected, Loopback1
```

```
ANCASH#sh ip route
……..<resultado omitido>……
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.23.0.0/21 is subnetted, 1 subnets
C       172.23.0.0 is directly connected, FastEthernet0/0
S    192.168.4.0/24 is directly connected, Serial0/0/0
    201.1.1.0/30 is subnetted, 1 subnets
C       201.1.1.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

```
AREQUIPA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 192.168.4.130 to network 0.0.0.0
   192.168.4.0/24 is variably subnetted, 5 subnets, 3 masks
C     192.168.4.0/27 is directly connected, FastEthernet0/0
C     192.168.4.32/27 is directly connected, FastEthernet0/1
R     192.168.4.64/28 [120/1] via 192.168.4.130, 00:00:04, Serial0/0/0
R     192.168.4.80/28 [120/1] via 192.168.4.130, 00:00:04, Serial0/0/0
C     192.168.4.128/30 is directly connected, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 192.168.4.130, 00:00:04, Serial0/0/0
```

VII. PRUEBAS DE VERIFICACION:

1. Realizamos, desde el router Arequipa, una prueba de conectividad normal hacia Internet, además de un ping extendido, empleando las direcciones de las FastEthernet.

```
AREQUIPA#ping 220.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 220.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/22 ms
AREQUIPA#ping 220.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 220.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/11 ms

AREQUIPA#ping
Protocol [ip]:
Target IP address: 220.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.4.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 220.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms

AREQUIPA#ping
Protocol [ip]:
Target IP address: 220.2.2.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.4.33
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
```

```
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 220.2.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.33
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/12 ms

AREQUIPA#ping 172.23.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.23.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/12/21 ms
AREQUIPA#
```

2. Desde un Host de la red del router Ancash realizamos una prueba de conectividad hacia Internet.

```
C:\Users\hector>ipconfig
Adaptador de Ethernet Conexión de área local:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 172.23.0.2
   Máscara de subred . . . . . . . . . . . . : 255.255.248.0
   Puerta de enlace predeterminada . . . . . : 172.23.0.1

C:\Users\hector>ping 192.168.1.1
Haciendo ping a 220.1.1.1 con 32 bytes de datos:
Respuesta desde 220.1.1.1: bytes=32 tiempo =38ms TTL=253
Respuesta desde 220.1.1.1: bytes=32 tiempo =15ms TTL=253
Respuesta desde 220.1.1.1: bytes=32 tiempo =13ms TTL=253
Respuesta desde 220.1.1.1: bytes=32 tiempo =25ms TTL=253
Estadísticas de ping para 220.1.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 13ms, Máximo = 38ms, Media = 22ms
```

3. Realizamos además un trazado de ruta hasta Internet.

```
C:\Users\hector>tracert 220.2.2..1
Traza a 220.2.2.1 sobre caminos de 30 saltos como máximo.

  1   9 ms     9 ms     8 ms     172.23.0.1
  2   12 ms    12 ms    13 ms    201.1.1.1
  3   17 ms    17 ms    15 ms    220.2.2.1
Traza completa.
```

4. Capturar la configuración de cada equipo.

OBSERVACIONES Y/O COMENTARIOS

_____

_____

Laboratorio N° 7 - EIGRP con rutas de distinto ancho de banda

INTRODUCCIÓN

Los routers EIGRP descubren a sus vecinos e intercambian paquetes de saludo. Se envían paquetes de saludo cada cinco segundos. Si no llegan tres, se da por hecho que el ruteador vecino está muerto y se utilizan rutas alternativas. EIGRP también envía actualizaciones incrementales acerca de cambios en la topología (cuando son necesarias).

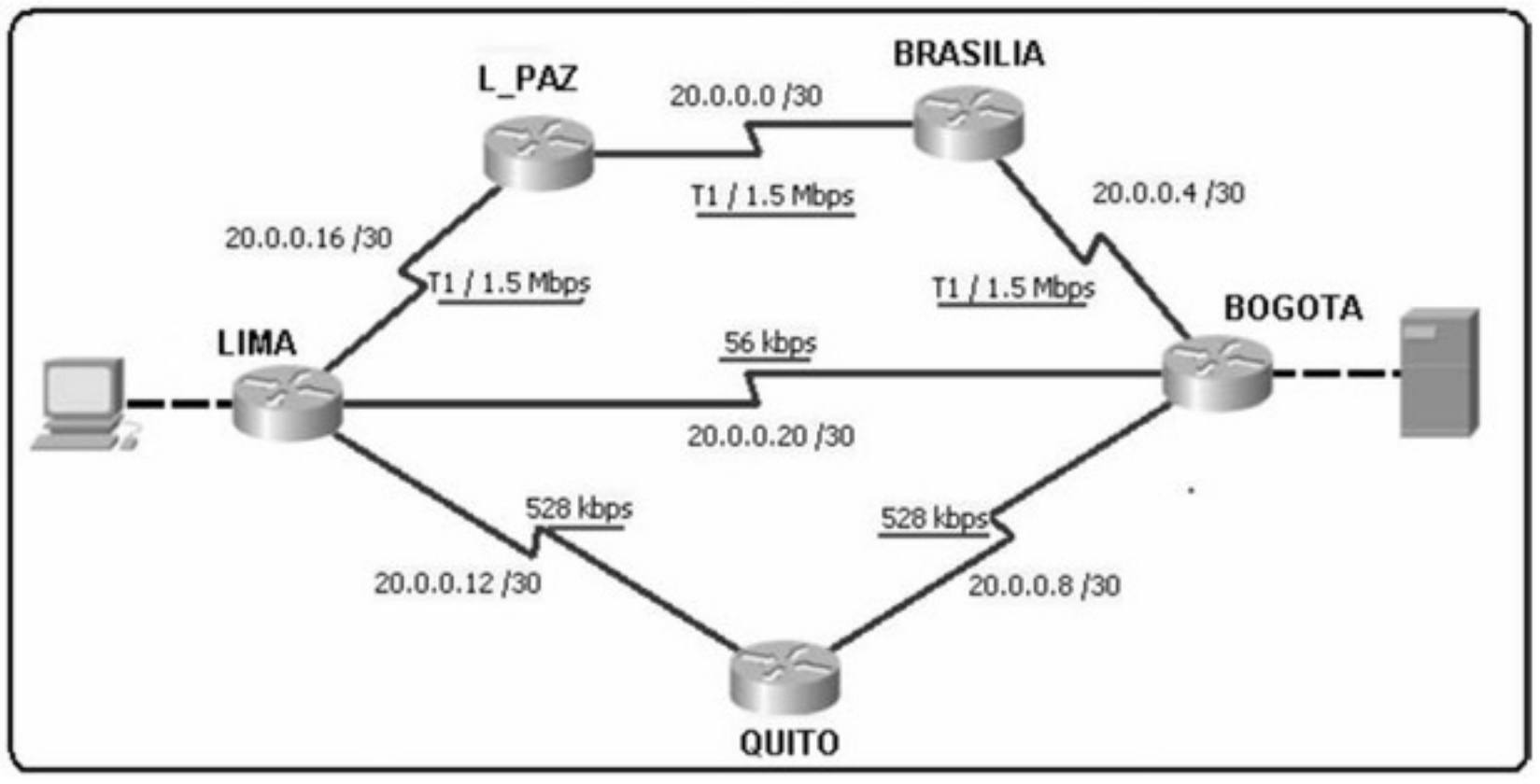
EIGRP llama "sucesor" al siguiente ruteador que está en su camino hacia un destino de red. El protocolo también se mantiene al tanto de los ruteadores de siguiente salto, denominados "sucesores factibles", los cuales pueden ofrecer rutas de respaldo carentes de ciclos.

OBJETIVOS

- Comprobación del funcionamiento del algoritmo DUAL en EIGRP.

DESCRIPCIÓN

EIGRP, con rutas de distinto ancho de banda, podrá utilizar las de menor velocidad como enlaces de backup. Todo el tráfico entre Lima y Bogotá se enruta vía L_Paz y Brasilia, ya que sus enlaces están configurados a 1544 Kb (por default) y, por lo tanto, la métrica EIGRP es más baja que en el resto de los enlaces: vía Quito, 512 Kb y directo, simulando Dial-Up, a 56 Kb.



DESARROLLO

1. Verifique el estado del router.
2. Si lo requiere el caso, elimine la configuración de cada router y reinícielo.
3. Habilite la opción de captura de texto en el Hyperterminal.
4. Realice la configuración básica de cada router con ayuda del bloc de notas.

5. Configuración de equipos:
   - El ancho de banda ha sido modificado para facilitar los enlaces backup para ciertos routers de acuerdo a su ubicación, pero habrá que considerar que el retardo se mantiene igual.

```
LIMA#sh interfaces S0/0/1
Serial0/1 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 20.0.0.17/30
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
……<resultado omitido>……..
```

```
LIMA#sh interfaces S0/0/0
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 20.0.0.22/30
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
……<resultado omitido>……..
```

6. Cada equipo presenta una configuración similar con el enrutamiento bajo EIGRP en el AS 62500, donde además se deshabilita la sumarización automática.

```
CONFIGURACIÓN FINAL
LIMA# SH RUN
!
!
!
interface FastEthernet0/0
 ip address 172.125.0.10 255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0
 bandwidth 56
 ip address 20.0.0.22 255.255.255.252
 clock rate 64000
!
!
interface Serial0/1
 bandwidth 512
 ip address 20.0.0.17 255.255.255.252
 clock rate 64000
!
interface Serial0/2
 ip address 20.0.0.13 255.255.255.252
 clock rate 64000
!
!
router eigrp 62500
 network 20.0.0.16 0.0.0.3
 network 20.0.0.12 0.0.0.3
 network 20.0.0.20 0.0.0.3
 network 172.125.0.0 0.0.0.255
 no auto-summary
!
!
```

```
L_PAZ#sh runn
!
!
interface Serial0/0
 ip address 20.0.0.18 255.255.255.252
!
interface Serial0/1
 ip address 20.0.0.2 255.255.255.252
 clock rate 64000
!
!
router eigrp 62500
 network 20.0.0.0 0.0.0.3
 network 20.0.0.16 0.0.0.3
 no auto-summary
!
!
```

```
BRASILIA#sh run
interface Serial0/0
 ip address 20.0.0.1 255.255.255.252
!
interface Serial0/1
 ip address 20.0.0.6 255.255.255.252
 clock rate 64000
!
!
router eigrp 62500
 network 20.0.0.0 0.0.0.3
 network 20.0.0.4 0.0.0.3
 no auto-summary
!
```

```
BOGOTÁ#sh run
!
!
interface FastEthernet0/0
 ip address 192.168.18.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0
 bandwidth 56
 ip address 20.0.0.21 255.255.255.252
!
interface Serial0/1
 ip address 20.0.0.5 255.255.255.252
!
interface Serial0/2
 bandwidth 528
 ip address 20.0.0.10 255.255.255.252
!
!
```

```
router eigrp 62500
 network 20.0.0.4 0.0.0.3
 network 20.0.0.8 0.0.0.3
 network 20.0.0.20 0.0.0.3
 network 192.168.18.0
 no auto-summary
!
```

```
QUITO#SH RUN
!
interface Serial0/0
 bandwidth 528
 ip address 20.0.0.14 255.255.255.252
!
interface Serial0/1
 bandwidth 528
 ip address 20.0.0.9 255.255.255.252
 clock rate 64000
!
!
router eigrp 62500
 network 20.0.0.12 0.0.0.3
 network 20.0.0.8 0.0.0.3
 no auto-summary
!
```

7. Es importante considerar siempre la revisión de la tabla de vecinos EIGRP de tal forma que se pueda comprobar la vecindad existente.

TABLA DE VECINOS:

```
LIMA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 62500
H   Address        Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   20.0.0.14      Se0/2        11   00:12:56 40     1000 0  17
1   20.0.0.18      Se0/1        14   00:12:23 40     1000 0  13
2   20.0.0.21      Se0/0        13   00:11:45 40     1000 0  26
```

```
L_PAZ#sh ip eigrp neighbors
IP-EIGRP neighbors for process 62500
H   Address        Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   20.0.0.17      Se0/0        14   00:15:15 40     1000 0  18
1   20.0.0.1       Se0/1        12   00:15:01 40     1000 0  21
```

8. TABLA TOPOLÓGICA

- Para el caso, las tablas topológicas están resumidas y sólo se muestran las redes que presentan rutas de respaldo en cada uno de los routers.
- Los routers Brasilia no presentan rutas de respaldo.

```
LIMA#sh ip eigrp topology
IP-EIGRP Topology Table for AS 62500
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 20.0.0.8/30, 1 successors, FD is 6896384
         via 20.0.0.18 (6896384/6384384), Serial0/1
         via 20.0.0.14 (11023872/5360384), Serial0/2
```

```
BOGOTÁ#sh ip eigrp topology
IP-EIGRP Topology Table for AS 62500
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 20.0.0.16/30, 1 successors, FD is 3193856
         via 20.0.0.6 (3193856/2681856), Serial0/1
         via 20.0.0.22 (46738176/2169856), Serial0/0
```

```
QUITO#sh ip eigrp topolo
IP-EIGRP Topology Table for AS 62500

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 192.168.18.0/24, 1 successors, FD is 5362944
         via 20.0.0.10 (5362944/28160), Serial0/1
         via 20.0.0.13 (6898944/3196416), Serial0/0
         via 20.0.0.13 (6898944/3196416), Serial0/0
P 20.0.0.20/30, 3 successors, FD is 46738176
         via 20.0.0.10 (46738176/46226176), Serial0/1
         via 20.0.0.13 (46738176/46226176), Serial0/0
         via 20.0.0.13 (46738176/46226176), Serial0/0
P 172.125.0.0/24, 1 successors, FD is 5362944
         via 20.0.0.13 (5362944/28160), Serial0/0
         via 20.0.0.10 (6898944/3196416), Serial0/1
P 20.0.0.4/30, 1 successors, FD is 5872384
         via 20.0.0.10 (5872384/2169856), Serial0/1
         via 20.0.0.13 (6896384/3193856), Serial0/0
         via 20.0.0.13 (6896384/3193856), Serial0/0
P 20.0.0.0/30, 3 successors, FD is 6384384
         via 20.0.0.10 (6384384/2681856), Serial0/1
         via 20.0.0.13 (6384384/2681856), Serial0/0
         via 20.0.0.13 (6384384/2681856), Serial0/0
P 20.0.0.16/30, 1 successors, FD is 5872384
         via 20.0.0.13 (5872384/2169856), Serial0/0
         via 20.0.0.10 (6896384/3193856), Serial0/1
```

9. TABLA DE ENRUTAMIENTO

- Para el caso se muestran las tablas de enrutamiento de todos los routers, para comprobar la aprensión de redes y su conexión.

```
LIMA#sh ip route
Gateway of last resort is not set

    20.0.0.0/30 is subnetted, 6 subnets
D      20.0.0.0 [90/2681856] via 20.0.0.18, 00:00:21, Serial0/1
D      20.0.0.4 [90/3193856] via 20.0.0.18, 00:00:21, Serial0/1
D      20.0.0.8 [90/6896384] via 20.0.0.18, 00:00:09, Serial0/1
C      20.0.0.12 is directly connected, Serial0/2
C      20.0.0.16 is directly connected, Serial0/1
C      20.0.0.20 is directly connected, Serial0/0
    172.125.0.0/24 is subnetted, 1 subnets
C      172.125.0.0 is directly connected, FastEthernet0/0
D   192.168.18.0/24 [90/3196416] via 20.0.0.18, 00:00:21, Serial0/1
```

```
L_PAZ#sh ip route
Gateway of last resort is not set
    20.0.0.0/30 is subnetted, 6 subnets
C      20.0.0.0 is directly connected, Serial0/1
D      20.0.0.4 [90/2681856] via 20.0.0.1, 00:19:57, Serial0/1
D      20.0.0.8 [90/6384384] via 20.0.0.1, 00:19:53, Serial0/1
D      20.0.0.12 [90/6896384] via 20.0.0.1, 00:01:09, Serial0/1
C      20.0.0.16 is directly connected, Serial0/0
D      20.0.0.20 [90/46738176] via 20.0.0.17, 00:04:25, Serial0/0
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/2172416] via 20.0.0.17, 00:04:25, Serial0/0
D   192.168.18.0/24 [90/2684416] via 20.0.0.1, 00:19:53, Serial0/1
```

```
BRASILIA#sh ip route
Gateway of last resort is not set
    20.0.0.0/30 is subnetted, 6 subnets
C      20.0.0.0 is directly connected, Serial0/0
C      20.0.0.4 is directly connected, Serial0/1
D      20.0.0.8 [90/5872384] via 20.0.0.5, 00:23:07, Serial0/1
D      20.0.0.12 [90/6384384] via 20.0.0.5, 00:04:23, Serial0/1
D      20.0.0.16 [90/2681856] via 20.0.0.2, 00:07:38, Serial0/0
D      20.0.0.20 [90/46738176] via 20.0.0.5, 00:23:07, Serial0/1
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/2684416] via 20.0.0.2, 00:07:38, Serial0/0
D   192.168.18.0/24 [90/2172416] via 20.0.0.5, 00:23:07, Serial0/1
```

```
BOGOTÁ#sh ip route
Gateway of last resort is not set
    20.0.0.0/30 is subnetted, 6 subnets
D      20.0.0.0 [90/2681856] via 20.0.0.6, 00:25:12, Serial0/1
C      20.0.0.4 is directly connected, Serial0/1
C      20.0.0.8 is directly connected, Serial0/2
D      20.0.0.12 [90/5872384] via 20.0.0.9, 00:06:28, Serial0/2
D      20.0.0.16 [90/3193856] via 20.0.0.6, 00:09:44, Serial0/1
C      20.0.0.20 is directly connected, Serial0/0
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/3196416] via 20.0.0.6, 00:09:44, Serial0/1
C   192.168.18.0/24 is directly connected, FastEthernet0/0
```

```
QUITO#sh ip route
Gateway of last resort is not set
    20.0.0.0/30 is subnetted, 6 subnets
D      20.0.0.0 [90/6384384] via 20.0.0.10, 00:24:44, Serial0/1
                [90/6384384] via 20.0.0.13, 00:06:12, Serial0/0
D      20.0.0.4 [90/5872384] via 20.0.0.10, 00:24:44, Serial0/1
C      20.0.0.8 is directly connected, Serial0/1
C      20.0.0.12 is directly connected, Serial0/0
D      20.0.0.16 [90/5872384] via 20.0.0.13, 00:06:13, Serial0/0
D      20.0.0.20 [90/46738176] via 20.0.0.10, 00:24:47, Serial0/1
                [90/46738176] via 20.0.0.13, 00:24:44, Serial0/0
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/5362944] via 20.0.0.13, 00:24:44, Serial0/0
D    192.168.18.0/24 [90/5362944] via 20.0.0.10, 00:24:47, Serial0/1
```

10. **DIAGNÓSTICO**

- Se realiza el diagnóstico de conectividad desde el Host del router Lima hacia el servidor en Bogotá.

```
PC>ping 192.168.18.2
Pinging 192.168.18.2 with 32 bytes of data:
Reply from 192.168.18.2: bytes=32 time=124ms TTL=124
Reply from 192.168.18.2: bytes=32 time=141ms TTL=124
Reply from 192.168.18.2: bytes=32 time=140ms TTL=124
Reply from 192.168.18.2: bytes=32 time=141ms TTL=124
Ping statistics for 192.168.18.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 124ms, Maximum = 141ms, Average = 136ms
```

- También se puede realizar un trazado de ruta para comprobar la conexión y los saltos que emplea. En este caso indica tres saltos desde su puerta de enlace.

```
PC>tracert 192.168.18.1
Tracing route to 192.168.18.1 over a maximum of 30 hops:
  1   31 ms    16 ms    31 ms    172.125.0.10
  2   32 ms    62 ms    63 ms    20.0.0.14
  3   109 ms   110 ms   109 ms   192.168.18.1
Trace complete.
PC>
```

11. **FALLA**

- Se simula la caída del enlace a Lima – L_Paz (1544 Kb) y automáticamente EIGRP conmuta vía Quito (512 Kb), a pesar de que el router Lima no tenia una ruta de respaldo hacia la red.
- El ping continuo cuando se produce el fallo indica que no se interrumpe completamente la comunicación, sólo se pierde un paquete.

```
PC>ping 192.168.18.2 -t
Pinging 192.168.18.2 with 32 bytes of data:
Reply from 192.168.18.2: bytes=32 time=83ms TTL=124
Reply from 192.168.18.2: bytes=32 time=156ms TTL=124
Reply from 192.168.18.2: bytes=32 time=123ms TTL=124
Reply from 192.168.18.2: bytes=32 time=125ms TTL=125
Reply from 192.168.18.2: bytes=32 time=109ms TTL=125
Request timed out.
Reply from 192.168.18.2: bytes=32 time=94ms TTL=125
Reply from 192.168.18.2: bytes=32 time=109ms TTL=125
Reply from 192.168.18.2: bytes=32 time=125ms TTL=125
Reply from 192.168.18.2: bytes=32 time=125ms TTL=125

Ping statistics for 192.168.18.2:
   Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
   Minimum = 83ms, Maximum = 203ms, Average = 123ms
```

12. TABLA DE ENRUTAMIENTO

- Después de la falla en el enlace de t1 Lima – La Paz es necesaria la revisión de la tabla de enrutamiento y comprobar las nuevas rutas, para el caso, sólo en los routers que transmitirán la conectividad del Host.

```
QUITO#sh ip route eigrp
    20.0.0.0/30 is subnetted, 5 subnets
D      20.0.0.0 [90/6384384] via 20.0.0.10, 00:37:41, Serial0/1
D      20.0.0.4 [90/5872384] via 20.0.0.10, 00:37:41, Serial0/1
D      20.0.0.20 [90/46738176] via 20.0.0.13, 00:38:37, Serial0/0
             [90/46738176] via 20.0.0.10, 00:37:39, Serial0/1
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/5362944] via 20.0.0.13, 00:28:12, Serial0/0
D    192.168.18.0/24 [90/5362944] via 20.0.0.10, 00:27:24, Serial0/1
```

```
LIMA#sh ip route eigrp
    20.0.0.0/30 is subnetted, 5 subnets
D      20.0.0.0 [90/47250176] via 20.0.0.21, 00:38:33, Serial0/0
D      20.0.0.4 [90/6384384] via 20.0.0.14, 00:38:35, Serial0/2
D      20.0.0.8 [90/5872384] via 20.0.0.14, 00:39:44, Serial0/2
    172.125.0.0/24 is subnetted, 1 subnets
D    192.168.18.0/24 [90/5874944] via 20.0.0.14, 00:28:18, Serial0/2
```

```
BOGOTÁ#sh ip route eigrp
    20.0.0.0/30 is subnetted, 5 subnets
D      20.0.0.0 [90/2681856] via 20.0.0.6, 00:39:15, Serial0/1
D      20.0.0.12 [90/46738176] via 20.0.0.22, 00:39:13, Serial0/0
    172.125.0.0/24 is subnetted, 1 subnets
D      172.125.0.0 [90/5874944] via 20.0.0.9, 00:01:48, Serial0/2
```

13. **PRUEBA**

- Finalmente se realiza un trazado de ruta con la que comprobaremos la nueva ruta obtenida por el router Lima.

```
PC>tracert 192.168.18.2
Tracing route to 192.168.18.2 over a maximum of 30 hops:
  1   48 ms    31 ms    31 ms    172.125.0.10
  2   48 ms    62 ms    63 ms    20.0.0.14
  3   62 ms    94 ms    78 ms    20.0.0.10
  4   110 ms   109 ms   125 ms   192.168.18.2
Trace complete.
```

CONCLUSIONES Y/U OBSERVACIONES

LABORATORIO N° 8 - EIGRP (análisis de DUAL)

DESCRIPCIÓN

EIGRP es un protocolo propietario de Cisco, que presenta una serie de ventajas a ser aprovechadas durante su proceso de enrutamiento, las cuales deben ser analizadas para facilidad de su entendimiento y aplicación.

Es conveniente analizar la configuración básica que se plantea para, más adelante, simplificar el entendimiento de sus opciones avanzadas.

OBJETIVOS

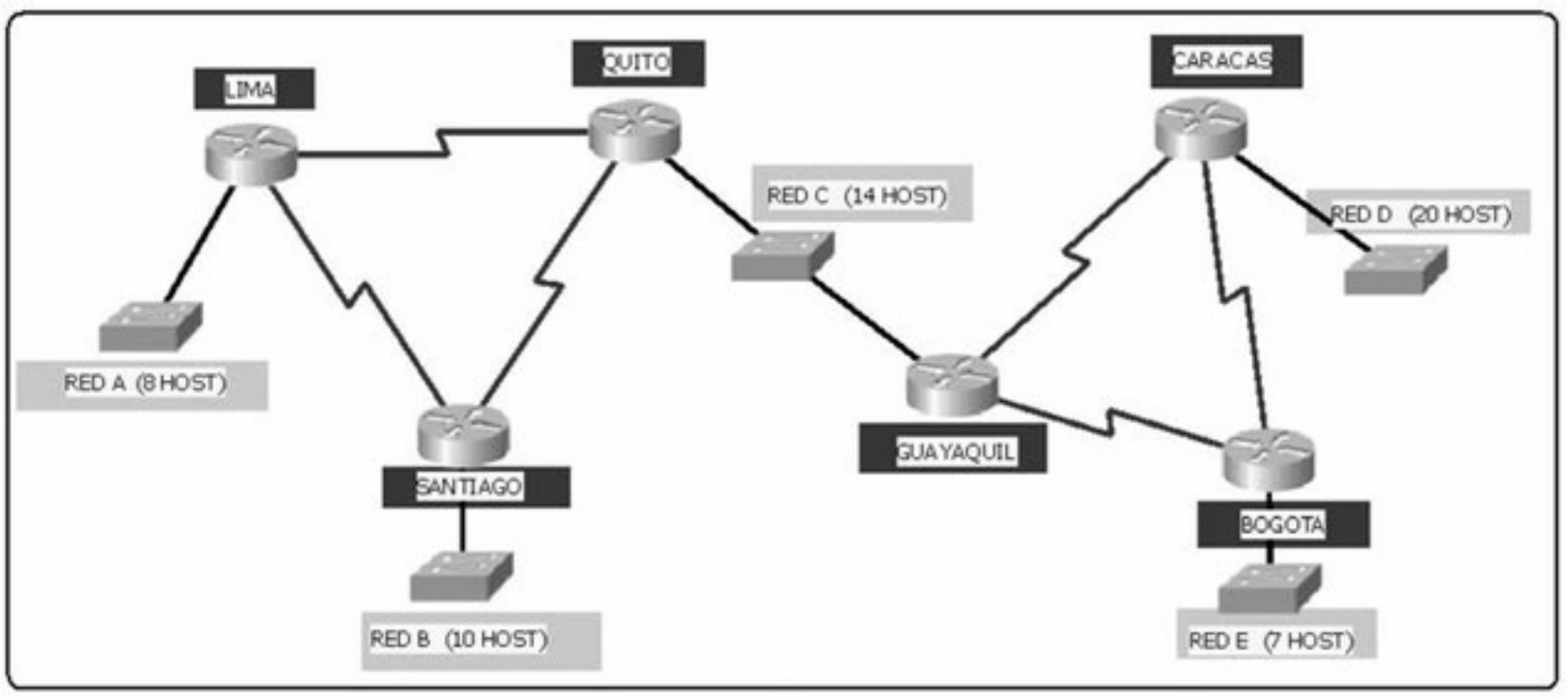
- Identificar el proceso de enrutamiento del protocolo EIGRP.
- Analizar la tabla topológica que EIGRP emplea en su enrutamiento.

PLANTEAMIENTO

Resolver el siguiente esquema de red, basándose en la implementación del protocolo EIGRP, considerando las opciones básicas de configuración que este protocolo plantea para facilitar el análisis de las tablas que componen su información de enrutamiento.

Asimismo, desarrolle el direccionamiento más adecuado para los requerimientos de cada red, empleando una dirección privada.

En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.



DESARROLLO

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

FASE I PASOS PREVIOS:

- Realice las conexiones y elimine la configuración de cada router, en caso la tenga.
- Habilite la opción de captura de texto en el Hyperterminal.
- Realice la configuración básica con ayuda del editor de texto.

FASE II Direccionamiento y configuración:

1. La tabla resume la solución de direccionamiento para cada red.

Denominación	N° HOST	IP	ID de red
Red A	8	16	192.168.8.32 /28
Red B	10	16	192.168.8.48 /28
Red C	14	16	192.168.8.64 /28
Red D	20	32	192.168.8.80 /27
Red E	7	16	192.168.8.96 /28
Lima - Santiago	2	4	192.168.8.112 /30
Lima – Quito	2	4	192.168.8.116 /30
Santiago - Quito	2	4	192.168.8.120 /30
Guayaquil – Bogotá	2	4	192.168.8.124 /30
Guayaquil – Caracas	2	4	192.168.8.128 /30
Bogotá – Caracas	2	4	192.168.8.132 /30

2. Enrutamiento EIGRP:
   a. Habilitamos el protocolo EIGRP dentro del AS 1, donde sólo se necesita mencionar la dirección general de red, ya que al colocar el comando **no auto-summary** se facilita que se publique individualmente cada una de la direcciones de subred.

```
CARACAS(config)#router eigrp 1
CARACAS(config-router)#no auto
CARACAS(config-router)#net 192.168.8.0
CARACAS(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.8.129 (Serial0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.8.133 (Serial0/0) is up: new adjacency
```

   b. Observaremos la identificación de vecinos mediante cada interfaz que recibe el mensaje, para el caso, los routers Caracas y Guayaquil.
   c. El comando de configuración del router eigrp log-neighbor-changes se encuentra activado de manera predeterminada en algunas implementaciones IOS. Si se encuentra activado, verá un resultado similar al mostrado para los routers.

```
GUAYAQUIL(config)# router eigrp 1
GUAYAQUIL(config-router)#no auto
GUAYAQUIL(config-router)#net 192.168.8.0
GUAYAQUIL(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.8.66 (FastEthernet0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.8.130 (Serial0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.8.125 (Serial0/1) is up: new adjacency
```

3. Tabla de vecinos EIGRP:
   a. Cada router debe identificar a sus vecinos directamente conectados, como se muestra en cada tabla:

```
CARACAS#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.133  Ser0/0       12  00:37:20 40    1000 0  63
1  192.168.8.129  Ser0/1       14  00:15:48 40    1000 0  25
```

```
BOGOTÁ#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.134  Ser0/0       11  00:37:50 40    1000 0  53
1  192.168.8.126  Ser0/1       12  00:16:19 40    1000 0  24
```

```
LIMA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.117  Ser0/1       12  00:38:09 40    1000 0  229
1  192.168.8.113  Ser0/0       14  00:38:00 40    1000 0  252
```

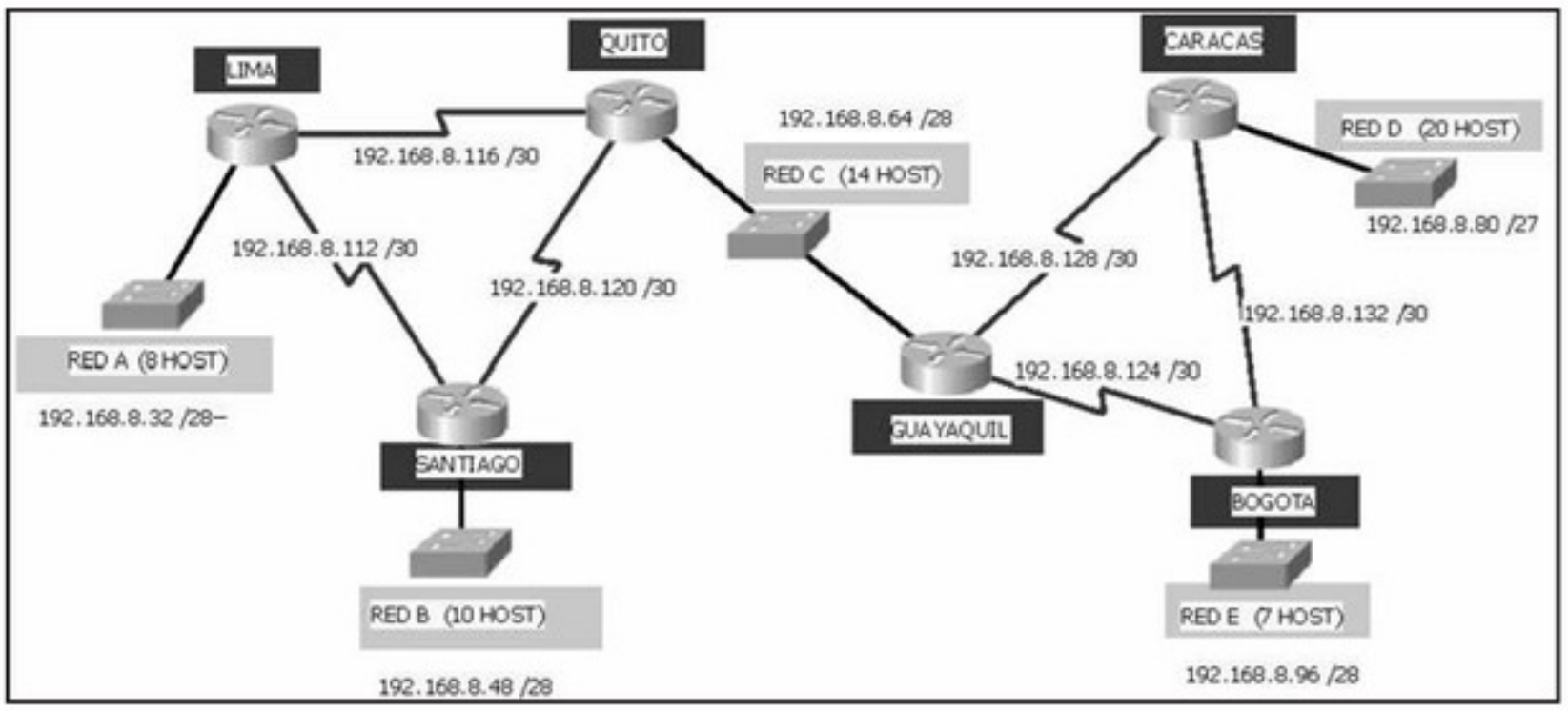
```
SANTIAGO#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.121  Ser0/1       12  00:38:34 40    1000 0  229
1  192.168.8.114  Ser0/0       13  00:38:34 40    1000 0  245
```

```
GUAYAQUIL#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.66   Fa0/0        13  00:18:15 40    1000 0  230
1  192.168.8.125  Ser0/1       14  00:18:12 40    1000 0  64
2  192.168.8.130  Ser0/0       11  00:18:12 40    1000 0  54
```

```
QUITO#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)        (ms)      Cnt Num
0  192.168.8.118  Ser0/0       12  00:40:03 40    1000 0  246
1  192.168.8.122  Ser0/1       13  00:39:50 40    1000 0  253
2  192.168.8.65   Fa0/0        12  00:18:48 40    1000 0  24
```

4. TABLA TOPOLÓGICA:

   a. Es creada posteriormente a la tabla de vecinos, con información publicada por cada router y replicada por los vecinos.



   b. El algoritmo DUAL es el encargado de analizar dicha información y establecer las rutas **SUCCESSOR** y **SUCCESSOR FACTIBLE**.

   c. **A continuación se presenta la tabla topológica del router Lima, que es analizada en cuanto al cálculo de su métrica**.

```
LIMA#sh ip eigrp topology
IP-EIGRP Topology Table for AS 1
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  r - Reply status
P 192.168.8.32/28, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 192.168.8.116/30, 1 successors, FD is 2169856
        via Connected, Serial0/1
P 192.168.8.112/30, 1 successors, FD is 2169856
        via Connected, Serial0/0
P 192.168.8.64/28, 1 successors, FD is 2172416
        via 192.168.8.117 (2172416/28160), Serial0/1
        via 192.168.8.113 (2684416/2172416), Serial0/0
P 192.168.8.120/30, 2 successors, FD is 2681856
        via 192.168.8.117 (2681856/2169856), Serial0/1
        via 192.168.8.113 (2681856/2169856), Serial0/0
P 192.168.8.48/28, 1 successors, FD is 2172416
        via 192.168.8.113 (2172416/28160), Serial0/0
        via 192.168.8.117 (2684416/2172416), Serial0/1
P 192.168.8.128/30, 1 successors, FD is 2684416
        via 192.168.8.117 (2684416/2172416), Serial0/1
        via 192.168.8.113 (4294967295/2684416), Serial0/0
P 192.168.8.124/30, 1 successors, FD is 2684416
        via 192.168.8.117 (2684416/2172416), Serial0/1
        via 192.168.8.113 (4294967295/2684416), Serial0/0
P 192.168.8.0/27, 1 successors, FD is 2686976
        via 192.168.8.117 (2686976/2174976), Serial0/1
        via 192.168.8.113 (4294967295/2686976), Serial0/0
P 192.168.8.132/30, 1 successors, FD is 3196416
        via 192.168.8.117 (3196416/2684416), Serial0/1
        via 192.168.8.113 (3708416/3196416), Serial0/0
P 192.168.8.96/28, 1 successors, FD is 2686976
        via 192.168.8.117 (2686976/2174976), Serial0/1
        via 192.168.8.113 (3198976/2686976), Serial0/0
```

- A continuación detallamos cada una de redes identificadas, con la **Tabla topológica detallada del router Lima**:

Red destino	INTERFAZ	N° RUTA	Métrica del router	Métrica desde el router vecino	FD	Tipo de ruta
P 192.168.8.32/28	FastEthernet0/0	1	28160	---	28160	S
P 192.168.8.112/30	Serial0/0	1	2169856	---	2169856	S
P 192.168.8.116/30	Serial0/1	1	2169856	---	2169856	S
P 192.168.8.64 /28	Serial0/1	1	2172416	28160	2172416	S
	Serial0/0	2	2684416	2172416	---	---
P 192.168.8.120/30	Serial0/1	1	2681856	2169856	2681856	S
	Serial0/0	2	2681856	2169856	2681856	S
P 192.168.8.48/28	Serial0/0	1	2172416	28160	2172416	S
	Serial0/1	2	2684416	2172416	---	---
P 192.168.8.128 /30	Serial0/1	1	2684416	2172416	2684416	S
	Serial0/0	2	4294967295	2684416	---	---
P 192.168.8.124 /30	Serial0/1	1	2684416	2172416	2681856	S
	Serial0/0	2	4294967295	2684416	---	---
P 192.168.8.132/30	Serial0/1	1	3196416	2684416	3196416	S
	Serial0/0	2	3708416	3196416	---	---
P 192.168.8.96 /28	Serial0/1	1	2686976	2172416	2686976	S
	Serial0/0	2	3198976	2686976	---	---
P 192.168.8.0 /27	Serial0/1	1	2686976	2174976	2686976	S
	Serial0/0	2	4294967295	2686976	---	---

- Tabla representativa de cada uno de los enlaces o saltos que debe tener cada ruta hacia la red destino, considerándose el ancho de banda a tomarse en cuenta para el cálculo de la métrica.

Red destino	Interfaz	N° RUTA	Enlaces (N° de saltos)					FD	Tipo de ruta
			Salto 1	Salto 2	Salto 3	Salto 4	Salto 5		
192.168.8.32/28	Fa0/0	1	Fa0/0					28160	S
192.168.8.112/30	S0/0	1	S0/0					2169856	S
192.168.8.116/30	S0/1	1	S0/1					2169856	S
192.168.8.64 /28	S0/1	1	T1	Fa				2172416	S
	S0/0	2	T1	T1	Fa			2684416	---
192.168.8.120/30	S0/1	1	T1	T1				2681856	S
	S0/0	2	T1	T1				2681856	S
192.168.8.48/28	S0/0	1	T1	Fa				2172416	S
	S0/1	2	T1	T1	Fa			2684416	---
192.168.8.128 /30	S0/1	1	T1	Fa	T1			2684416	S
	S0/0	2	T1	T1	Fa	T1		4294967295	---
192.168.8.124 /30	S0/1	1	T1	Fa	T1			2684416	S
	S0/0	2	T1	T1	Fa	T1		4294967295	---
192.168.8.132/30	S0/1	1	T1	fa	T1	T1		3196416	S
	S0/0	2	T1	T1	Fa	T1	T1	3708416	---
192.168.8.96 /28	S0/1	1	T1	Fa	T1	Fa		2686976	S
	S0/0	2	T1	T1	Fa	T1	Fa	3198976	---
192.168.8.0 /27	S0/1	1	T1	Fa	T1	Fa		2686976	S
	S0/0	2	T1	T1	Fa	T1	Fa	4294967295	---

1. La formula del algoritmo se basa en emplear el ancho de banda más bajo de todos los enlaces, más la sumatoria de retardos en cada enlace.

$$\frac{10000000}{\text{(BW menor)}} \times 256 = A \qquad \frac{\text{(suma de retardos)}}{10} \times 256 = B$$

$$A + B = METRICA$$

2. Así, por ejemplo, para llegar a la red 192.168.8.64 /28 se tienen dos rutas vía s0/0 y s0/1,
   - La métrica vía s0/1 es 2172416, pasando por la interfaz serial y luego la interfaz FastEthernet (según tabla y grafico).
   - Dado que el ancho de banda más bajo está en la interfaz serial (T1=1544 kbps.) y los retardos de cada uno son 20000useg y 100useg, el resultado se obtendrá de la siguiente manera:

$$\frac{10000000}{1544} \times 256 = 1658031.1 \qquad \frac{(20000+100)}{10} \times 256 = 514560$$

$$1658031.1 + 514560 = 2172591$$

   - Se aprecia una mínima diferencia por la precisión del cálculo en la operación.

3. Ejemplo 2. Para llegar a la red 192.168.8.132 /30 se tienen dos rutas: vía s0/0 y s0/1.
   - La métrica vía s0/1 es 3196416, pasando por tres enlaces con interfaz serial y uno, mediante interfaz FastEthernet (según tabla y gráfico).
   - Dado que el ancho de banda más bajo está en la interfaz serial (T1=1544 kbps.) y los retardos de cada uno son 20000useg, 20000useg, 20000useg y 100useg, se obtendrá de la siguiente manera el resultado:

$$\frac{10000000}{1544} \times 256 = 1658031.1 \qquad \frac{(60000+100)}{10} \times 256 = 1538560$$

$$1658031.1 + 1538560 = 3196591.1$$

5. **TABLA TOPOLÓGICA**:
   - Cada router, de acuerdo a su ubicación, presentara una métrica, además de emplear rutas SUCESSOR o rutas SUCESSOR FACTIBLE.
   - Para comparar con la tabla topológica del router Lima, se presenta la tabla del router Guayaquil.

```
GUAYAQUIL#sh ip eigrp topol
IP-EIGRP Topology Table for AS 1
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

P 192.168.8.64/28, 1 successors, FD is 28160
      via Connected, FastEthernet0/0
P 192.168.8.128/30, 1 successors, FD is 2169856
      via Connected, Serial0/0
P 192.168.8.124/30, 1 successors, FD is 2169856
      via Connected, Serial0/1
P 192.168.8.0/27, 1 successors, FD is 2172416
      via 192.168.8.130 (2172416/28160), Serial0/0
      via 192.168.8.125 (2684416/2172416), Serial0/1
P 192.168.8.132/30, 2 successors, FD is 2681856
      via 192.168.8.130 (2681856/2169856), Serial0/0
      via 192.168.8.125 (2681856/2169856), Serial0/1
P 192.168.8.96/28, 1 successors, FD is 2172416
      via 192.168.8.125 (2172416/28160), Serial0/1
      via 192.168.8.130 (2684416/2172416), Serial0/0
P 192.168.8.116/30, 1 successors, FD is 2172416
      via 192.168.8.66 (2172416/2169856), FastEthernet0/0
P 192.168.8.120/30, 1 successors, FD is 2172416
      via 192.168.8.66 (2172416/2169856), FastEthernet0/0
P 192.168.8.32/28, 1 successors, FD is 2174976
      via 192.168.8.66 (2174976/2172416), FastEthernet0/0
P 192.168.8.112/30, 1 successors, FD is 2684416
      via 192.168.8.66 (2684416/2681856), FastEthernet0/0
P 192.168.8.48/28, 1 successors, FD is 2174976
      via 192.168.8.66 (2174976/2172416), FastEthernet0/0
```

6. TABLA DE ENRUTAMIENTO:
   a. Cada router presenta sólo las rutas **Successor** hacia sus diferentes redes de acuerdo a las rutas analizadas mediante DUAL.

```
CARACAS#sh ip route
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.32/28 [90/2686976] via 192.168.8.129, 00:06:56, Serial0/1
D      192.168.8.48/28 [90/2686976] via 192.168.8.129, 00:06:47, Serial0/1
C      192.168.8.0/27 is directly connected, FastEthernet0/0
D      192.168.8.64/28 [90/2172416] via 192.168.8.129, 00:07:25, Serial0/1
D      192.168.8.96/28 [90/2172416] via 192.168.8.133, 00:07:16, Serial0/0
D      192.168.8.112/30 [90/3196416] via 192.168.8.129, 00:06:56, Serial0/1
D      192.168.8.116/30 [90/2684416] via 192.168.8.129, 00:07:25, Serial0/1
D      192.168.8.120/30 [90/2684416] via 192.168.8.129, 00:07:25, Serial0/1
D      192.168.8.124/30 [90/2681856] via 192.168.8.129, 00:07:25, Serial0/1
                        [90/2681856] via 192.168.8.133, 00:07:16, Serial0/0
C      192.168.8.128/30 is directly connected, Serial0/1
C      192.168.8.132/30 is directly connected, Serial0/0
CARACAS#
```

```
BOGOTÁ#sh ip route
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.0/27 [90/2172416] via 192.168.8.134, 00:08:03, Serial0/0
D      192.168.8.32/28 [90/2686976] via 192.168.8.126, 00:07:42, Serial0/1
D      192.168.8.48/28 [90/2686976] via 192.168.8.126, 00:07:34, Serial0/1
D      192.168.8.64/28 [90/2172416] via 192.168.8.126, 00:07:59, Serial0/1
C      192.168.8.96/28 is directly connected, FastEthernet0/0
D      192.168.8.112/30 [90/3196416] via 192.168.8.126, 00:07:42, Serial0/1
D      192.168.8.116/30 [90/2684416] via 192.168.8.126, 00:07:59, Serial0/1
D      192.168.8.120/30 [90/2684416] via 192.168.8.126, 00:07:59, Serial0/1
C      192.168.8.124/30 is directly connected, Serial0/1
D      192.168.8.128/30 [90/2681856] via 192.168.8.134, 00:08:03, Serial0/0
                        [90/2681856] via 192.168.8.126, 00:07:59, Serial0/1
C      192.168.8.132/30 is directly connected, Serial0/0
```

```
GUAYAQUIL#SH IP ROUT
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.0/27 [90/2172416] via 192.168.8.130, 00:00:55, Serial0/0
D      192.168.8.32/28 [90/2174976] via 192.168.8.66, 00:00:25, FastEthernet0/0
D      192.168.8.48/28 [90/2174976] via 192.168.8.66, 00:00:17, FastEthernet0/0
C      192.168.8.64/28 is directly connected, FastEthernet0/0
D      192.168.8.96/28 [90/2172416] via 192.168.8.125, 00:00:42, Serial0/1
D      192.168.8.112/30 [90/2684416] via 192.168.8.66, 00:00:25, FastEthernet0/0
D      192.168.8.116/30 [90/2172416] via 192.168.8.66, 00:01:09, FastEthernet0/0
D      192.168.8.120/30 [90/2172416] via 192.168.8.66, 00:01:09, FastEthernet0/0
C      192.168.8.124/30 is directly connected, Serial0/1
C      192.168.8.128/30 is directly connected, Serial0/0
D      192.168.8.132/30 [90/2681856] via 192.168.8.130, 00:00:55, Serial0/0
                        [90/2681856] via 192.168.8.125, 00:00:42, Serial0/1
```

```
LIMA#sh ip route
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.0/27 [90/2686976] via 192.168.8.117, 00:08:48, Serial0/1
C      192.168.8.32/28 is directly connected, FastEthernet0/0
D      192.168.8.48/28 [90/2172416] via 192.168.8.113, 00:08:40, Serial0/0
D      192.168.8.64/28 [90/2172416] via 192.168.8.117, 00:08:48, Serial0/1
D      192.168.8.96/28 [90/2686976] via 192.168.8.117, 00:08:48, Serial0/1
C      192.168.8.112/30 is directly connected, Serial0/0
C      192.168.8.116/30 is directly connected, Serial0/1
D      192.168.8.120/30 [90/2681856] via 192.168.8.117, 00:08:48, Serial0/1
                        [90/2681856] via 192.168.8.113, 00:08:40, Serial0/0
D      192.168.8.124/30 [90/2684416] via 192.168.8.117, 00:08:48, Serial0/1
D      192.168.8.128/30 [90/2684416] via 192.168.8.117, 00:08:48, Serial0/1
D      192.168.8.132/30 [90/3196416] via 192.168.8.117, 00:08:48, Serial0/1
```

```
SANTIAGO#sh ip route
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.0/27 [90/2686976] via 192.168.8.121, 00:09:27, Serial0/1
D      192.168.8.32/28 [90/2172416] via 192.168.8.114, 00:09:27, Serial0/0
C      192.168.8.48/28 is directly connected, FastEthernet0/0
D      192.168.8.64/28 [90/2172416] via 192.168.8.121, 00:09:27, Serial0/1
D      192.168.8.96/28 [90/2686976] via 192.168.8.121, 00:09:27, Serial0/1
C      192.168.8.112/30 is directly connected, Serial0/0
D      192.168.8.116/30 [90/2681856] via 192.168.8.121, 00:09:27, Serial0/1
                        [90/2681856] via 192.168.8.114, 00:09:27, Serial0/0
C      192.168.8.120/30 is directly connected, Serial0/1
D      192.168.8.124/30 [90/2684416] via 192.168.8.121, 00:09:27, Serial0/1
D      192.168.8.128/30 [90/2684416] via 192.168.8.121, 00:09:27, Serial0/1
D      192.168.8.132/30 [90/3196416] via 192.168.8.121, 00:09:27, Serial0/1
```

```
QUITO#sh ip route
……..< resultado omitido >……..
Gateway of last resort is not set
    192.168.8.0/24 is variably subnetted, 11 subnets, 3 masks
D      192.168.8.0/27 [90/2174976] via 192.168.8.65, 00:10:42, FastEthernet0/0
D      192.168.8.32/28 [90/2172416] via 192.168.8.118, 00:10:13, Serial0/0
D      192.168.8.48/28 [90/2172416] via 192.168.8.122, 00:10:04, Serial0/1
C      192.168.8.64/28 is directly connected, FastEthernet0/0
D      192.168.8.96/28 [90/2174976] via 192.168.8.65, 00:10:29, FastEthernet0/0
D      192.168.8.112/30 [90/2681856] via 192.168.8.118, 00:10:13, Serial0/0
                        [90/2681856] via 192.168.8.122, 00:10:04, Serial0/1
C      192.168.8.116/30 is directly connected, Serial0/0
C      192.168.8.120/30 is directly connected, Serial0/1
D      192.168.8.124/30 [90/2172416] via 192.168.8.65, 00:10:56, FastEthernet0/0
D      192.168.8.128/30 [90/2172416] via 192.168.8.65, 00:10:56, FastEthernet0/0
D      192.168.8.132/30 [90/2684416] via 192.168.8.65, 00:10:42, FastEthernet0/0
```

FASE III: TAREAS:

- Deshabilite el resumen automático en el enrutamiento EIGRP y verifique la modificación de las tablas topológica y de enrutamiento.
- Habilite nuevamente la opción de resumen automático.

FASE IV

- Capture la información de cada router:
  a. Tabla de vecinos.
  b. Tabla de topología.
  c. Tabla de enrutamiento.
  d. Configuración activa.

OBSERVACIONES Y/O COMENTARIOS

_____

LABORATORIO N° 9 - EIGRP y redistribución de rutas estáticas

DESCRIPCIÓN

La redistribución es un proceso de traducción de rutas desde un protocolo hacia otro o también desde un enrutamiento estático hacia uno dinámico.

Lo que se hace con los comandos **redistribute** es que todas las rutas que han sido aprendidas mediante una ruta estática o dinámica ahora sean conocidas por el protocolo EIGRP. Combinando los comandos se podrá hacer un posible filtrado y manejo de rutas entre protocolos distintos, de esta forma, un router tiene la capacidad de pasar información de un protocolo de enrutamiento hacia otro.

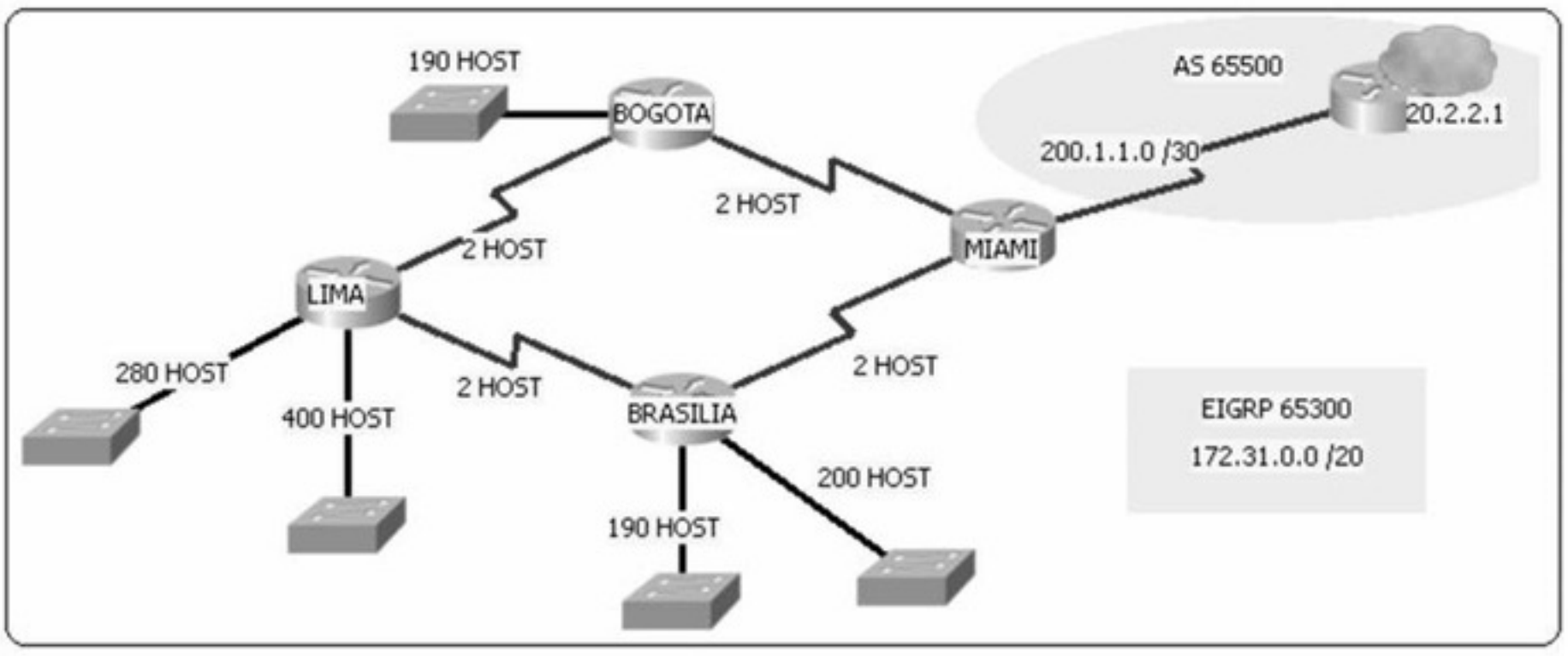
OBJETIVOS

- Redistribución de rutas estáticas en el enrutamiento EIGRP.
- Analizar la tabla topológica que EIGRP emplea en su enrutamiento.

PLANTEAMIENTO

En el siguiente esquema de red se plantea la necesidad de que una red en un AS 65300 con el protocolo EIGRP se conecte a Internet mediante el AS 65500, considerando que se redistribuirán rutas estáticas y se publicarán redes sumarizadas manualmente.

En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.



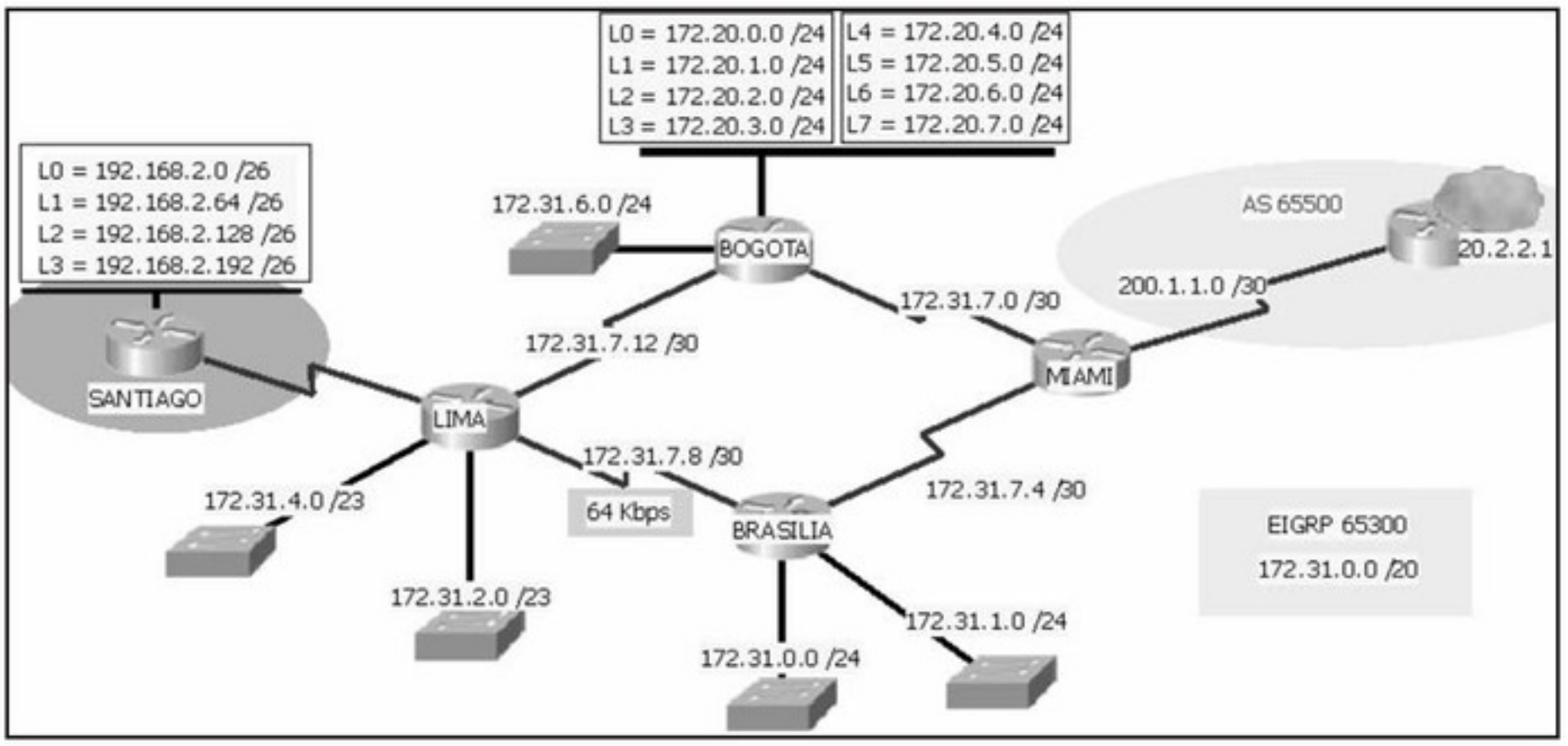
1. Resolver el direccionamiento por VLSM a partir de la dirección 172.31.0.0 /20.
2. Configurar las opciones básicas de cada router.
3. Habilitar el enrutamiento EIGRP, según las características de la red con las rutas internas y externas.
4. El enlace entre Lima y Brasilia es de 64 Kbps y para el resto de conexiones seriales será de 1544 kbps (T1).
5. Realizar las pruebas de conectividad a cada punto.

6. Capturar la siguiente información:
   - Configuración activa.
   - Tabla de vecinos (indique los detalles de la información mostrada).
   - Tabla topológica (indique los tipos de ruta).
   - Tabla de enrutamiento (indique las rutas de nivel 1, 2 ó rutas principales y secundarias).
7. Agregar el router Santiago, que presenta 4 subredes de 60 Hosts cada una, pero no considerarlo dentro del enrutamiento EIGRP.
8. Agregar 8 subredes de 200 Hosts al router BOGOTÁ y sumarizar manualmente para su publicación en la red.
9. Verificar las rutas internas y externas EIGRP.
10. Verificar la conectividad y el acceso remoto a cada router.
11. Capturar la siguiente información:
    - Configuración activa.
    - Tabla topológica.
    - Tabla de vecinos.
    - Tabla de enrutamiento.

DESARROLLO

FASE I:

1. La solución al direccionamiento se presenta en el siguiente esquema de red, empleando además una dirección publica (199.1.1.0 /30) para el enlace entre Lima y Santiago.



2. Configuración del router MIAMI:

   Se habilitará el enrutamiento EIGRP, desactivando el resumen automático; luego habilitamos la ruta por defecto y finalmente se redistribuye para su publicación dentro de EIGRP.

   El resumen automático elimina la ruta resumida Null0 y permite a EIGRP buscar una ruta por defecto o de superred cuando una ruta secundaria EIGRP no coincida con un paquete de destino.

```
MIAMI#SH RUN
Building configuration...
Current configuration : 1706 bytes
!
hostname MIAMI
!
……..<resultado omitido>…….
!
interface Serial0/0/0
 ip address 172.31.7.2 255.255.255.252
!
interface Serial0/0/1
 ip address 200.1.1.1 255.255.255.0
!
interface Serial0/1/0
 ip address 172.31.7.6 255.255.255.252
!
……..<resultado omitido>…….
!
router eigrp 65300
 redistribute static
 network 172.31.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
End
```

3. Habilitado el enrutamiento se muestra la tabla de vecinos EIGRP de cada router:

```
BRASILIA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 65300
H   Address        Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   172.31.7.10    Ser0/0/1      15  00:50:07  40    1000  0  229
1   172.31.7.6     Ser0/0/0      14  00:50:07  40    1000  0  179
```

```
LIMA#sh ip eigrp ne
IP-EIGRP neighbors for process 65300
H   Address        Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   172.31.7.9     Ser0/0/1      12  00:50:30  40    1000  0  252
1   172.31.7.14    Ser0/0/0      12  00:50:29  40    1000  0  169
```

```
BOGOTÁ#sh ip eigrp neighbors
IP-EIGRP neighbors for process 65300
H   Address        Interface    Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   172.31.7.2     Ser0/0/0      14  00:52:12  40    1000  0  180
1   172.31.7.13    Ser0/0/1      13  00:52:07  40    1000  0  228
```

```
MIAMI# sh ip eigrp neighbors
IP-EIGRP neighbors for process 65300
H  Address      Interface    Hold Uptime   SRTT  RTO  Q  Seq
                              (sec)       (ms)       Cnt Num
0  172.31.7.5   Ser0/1/0      13 00:52:59 40    1000 0  253
1  172.31.7.1   Ser0/0/0      13 00:52:59 40    1000 0  167
```

4. TABLA TOPOLÓGICA:

- EIGRP emplea el enlace con el ancho de banda más lento para calcular la métrica compuesta. El enlace más lento es el enlace de 64 Kbps (Lima – Brasilia) que contiene la red 172.31.7.8/30. En este ejemplo, los enlaces de 1544 Mbps son irrelevantes en el cálculo en lo que respecta a la métrica del ancho de banda.
- Para ciertas rutas existirán rutas de respaldo (**Successor factible)**, que son de métrica más baja desde el vecino a la red destino, en comparación con la del mismo router.

```
LIMA#show ip eigrp topology
IP-EIGRP Topology Table for AS 65300
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  r - Reply status
P 172.31.4.0/23, 1 successors, FD is 28160
      via Connected, FastEthernet0/1
P 172.31.2.0/23, 1 successors, FD is 28160
      via Connected, FastEthernet0/0
P 172.31.7.8/30, 1 successors, FD is 40512000
      via Connected, Serial0/0/1
P 172.31.7.12/30, 1 successors, FD is 2169856
      via Connected, Serial0/0/0
P 172.31.7.0/30, 1 successors, FD is 2681856
      via 172.31.7.14 (2681856/2169856), Serial0/0/0
      via 172.31.7.9 (41536000/2681856), Serial0/0/1
P 0.0.0.0/0, 1 successors, FD is 3193856
      via 172.31.7.14 (3193856/2681856), Serial0/0/0
      via 172.31.7.9 (41536000/2681856), Serial0/0/1   ← Successor factible
P 172.31.0.0/24, 1 successors, FD is 3196416
      via 172.31.7.14 (3196416/2684416), Serial0/0/0
      via 172.31.7.9 (4294967295/28160), Serial0/0/1   ← Successor factible
P 172.31.1.0/24, 1 successors, FD is 3196416
      via 172.31.7.14 (3196416/2684416), Serial0/0/0
      via 172.31.7.9 (4294967295/28160), Serial0/0/1   ← Successor factible
P 172.31.7.4/30, 1 successors, FD is 3193856
      via 172.31.7.14 (3193856/2681856), Serial0/0/0
      via 172.31.7.9 (4294967295/2169856), Serial0/0/1← Successor factible
```

- Brasilia presenta tres rutas de respaldo, por su ubicación y la velocidad de enlace que presenta su router vecino hacia la red de destino.

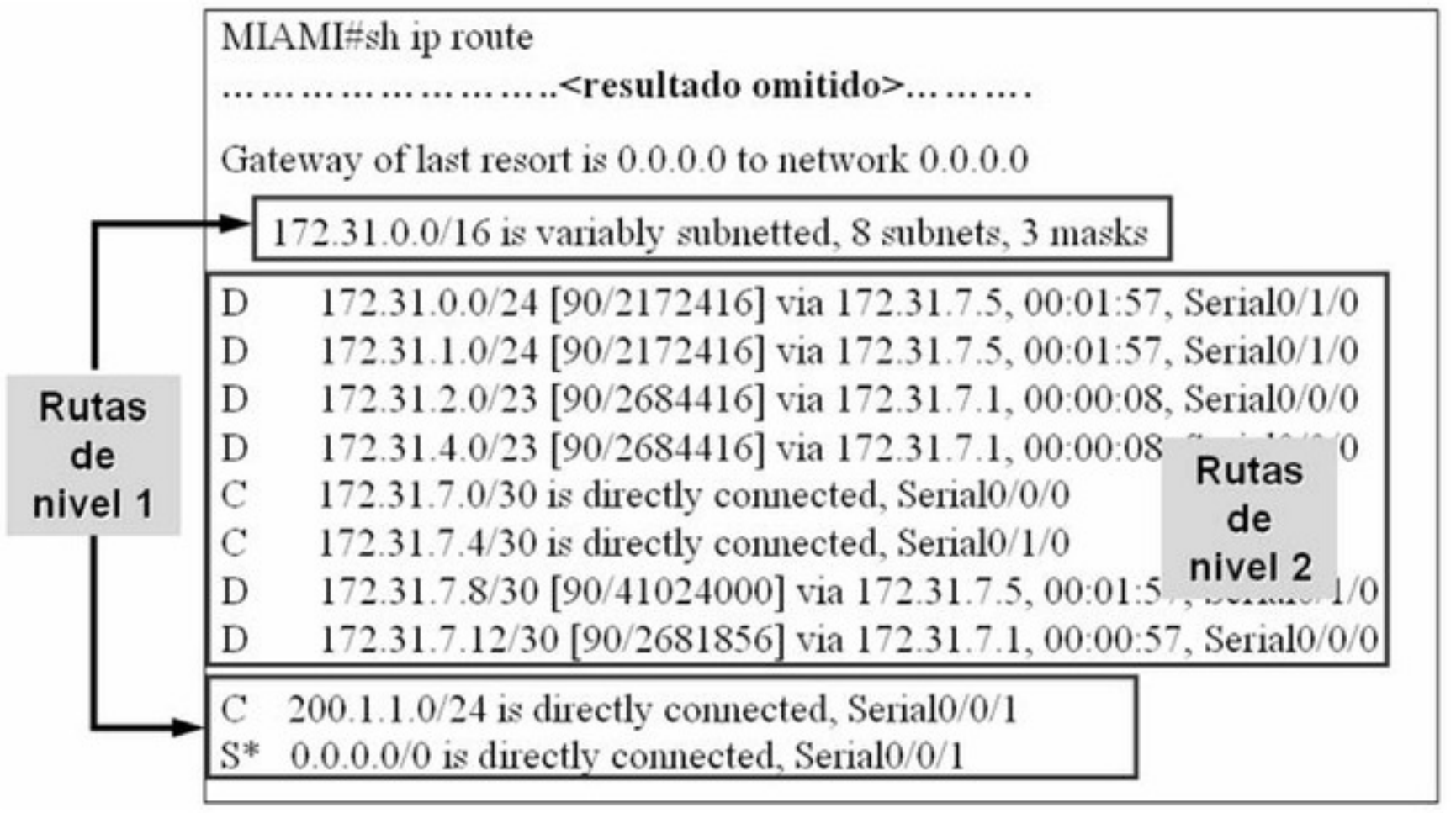
```
BRASILIA#sh ip eigrp topology
IP-EIGRP Topology Table for AS 65300
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

P 172.31.0.0/24, 1 successors, FD is 28160
      via Connected, FastEthernet0/0
P 172.31.1.0/24, 1 successors, FD is 28160
      via Connected, FastEthernet0/1
P 172.31.7.8/30, 1 successors, FD is 40512000
      via Connected, Serial0/0/1
P 172.31.7.4/30, 1 successors, FD is 2169856
      via Connected, Serial0/0/0
P 172.31.2.0/23, 1 successors, FD is 3196416
      via 172.31.7.6 (3196416/2684416), Serial0/0/0
      via 172.31.7.10 (4294967295/28160), Serial0/0/1   ← Successor factible
P 172.31.4.0/23, 1 successors, FD is 3196416
      via 172.31.7.6 (3196416/2684416), Serial0/0/0
      via 172.31.7.10 (4294967295/28160), Serial0/0/1   ← Successor factible
P 172.31.7.12/30, 1 successors, FD is 3193856
      via 172.31.7.6 (3193856/2681856), Serial0/0/0
      via 172.31.7.10 (4294967295/2169856), Serial0/0/1← Successor factible
P 172.31.7.0/30, 1 successors, FD is 2681856
      via 172.31.7.6 (2681856/2169856), Serial0/0/0
      via 172.31.7.10 (4294967295/2681856), Serial0/0/1
P 0.0.0.0/0, 1 successors, FD is 2681856
      via 172.31.7.6 (2681856/2169856), Serial0/0/0
```

- La tabla topológica de los routers siguientes no presentan successor factible, por su ubicación.

```
MIAMI#sh ip eigrp topology
IP-EIGRP Topology Table for AS 65300
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

P 172.31.7.0/30, 1 successors, FD is 2169856
      via Connected, Serial0/0/0
P 0.0.0.0/0, 1 successors, FD is 2169856
      via Rstatic (2169856/0)
P 172.31.7.12/30, 1 successors, FD is 2681856
      via 172.31.7.1 (2681856/2169856), Serial0/0/0
P 172.31.2.0/23, 1 successors, FD is 2684416
      via 172.31.7.1 (2684416/2172416), Serial0/0/0
P 172.31.4.0/23, 1 successors, FD is 2684416
      via 172.31.7.1 (2684416/2172416), Serial0/0/0
P 172.31.7.8/30, 1 successors, FD is 41024000
      via 172.31.7.5 (41024000/40512000), Serial0/1/0
      via 172.31.7.1 (4294967295/41024000), Serial0/0/0
P 172.31.0.0/24, 1 successors, FD is 2172416
      via 172.31.7.5 (2172416/28160), Serial0/1/0
P 172.31.1.0/24, 1 successors, FD is 2172416
      via 172.31.7.5 (2172416/28160), Serial0/1/0
P 172.31.7.4/30, 1 successors, FD is 2169856
      via Connected, Serial0/1/0
```

```
BOGOTA#show ip eigrp topology
IP-EIGRP Topology Table for AS 65300
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

P 172.31.7.0/30, 1 successors, FD is 2169856
      via Connected, Serial0/0/0
P 172.31.7.12/30, 1 successors, FD is 2169856
      via Connected, Serial0/0/1
P 172.31.2.0/23, 1 successors, FD is 2172416
      via 172.31.7.13 (2172416/28160), Serial0/0/1
P 172.31.4.0/23, 1 successors, FD is 2172416
      via 172.31.7.13 (2172416/28160), Serial0/0/1
P 0.0.0.0/0, 1 successors, FD is 2681856
      via 172.31.7.2 (2681856/2169856), Serial0/0/0
P 172.31.7.8/30, 1 successors, FD is 41024000
      via 172.31.7.13 (41024000/40512000), Serial0/0/1
      via 172.31.7.2 (41536000/41024000), Serial0/0/0
P 172.31.0.0/24, 1 successors, FD is 2684416
      via 172.31.7.2 (2684416/2172416), Serial0/0/0
P 172.31.1.0/24, 1 successors, FD is 2684416
      via 172.31.7.2 (2684416/2172416), Serial0/0/0
P 172.31.7.4/30, 1 successors, FD is 2681856
      via 172.31.7.2 (2681856/2169856), Serial0/0/0
```

5. Analizamos las rutas de nivel 1 y nivel 2 en cada tabla de enrutamiento.
   - Las rutas internas, como se conocen a las redes dentro del AS, y las externas, son rutas resumidas o redistribuidas.
   - Hasta el momento sólo existirá publicada una ruta externa etiquetada como D*EX, que viene a ser la ruta por defecto redistribuida por el router Miami.


MIAMI#sh ip route
……..<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D 172.31.0.0/24 [90/2172416] via 172.31.7.5, 00:01:57, Serial0/1/0
D 172.31.1.0/24 [90/2172416] via 172.31.7.5, 00:01:57, Serial0/1/0
D 172.31.2.0/23 [90/2684416] via 172.31.7.1, 00:00:08, Serial0/0/0
D 172.31.4.0/23 [90/2684416] via 172.31.7.1, 00:00:08
C 172.31.7.0/30 is directly connected, Serial0/0/0
C 172.31.7.4/30 is directly connected, Serial0/1/0
D 172.31.7.12/30 [90/2681856] via 172.31.7.1, 00:00:57, Serial0/0/0
C 200.1.1.0/24 is directly connected, Serial0/0/1
S* 0.0.0.0/0 is directly connected, Serial0/0/1
Rutas de nivel 1
Rutas de nivel 2

- En los siguientes routers se muestra la ruta externa:

```
BRASILIA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 172.31.7.6 to network 0.0.0.0
172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
C       172.31.0.0/24 is directly connected, FastEthernet0/0
C       172.31.1.0/24 is directly connected, FastEthernet0/1
D       172.31.2.0/23 [90/3196416] via 172.31.7.6, 00:00:07, Serial0/0/0
D       172.31.4.0/23 [90/3196416] via 172.31.7.6, 00:00:07, Serial0/0/0
D       172.31.7.0/30 [90/2681856] via 172.31.7.6, 00:00:11,
C       172.31.7.4/30 is directly connected, Serial0/0/0
C       172.31.7.8/30 is directly connected, Serial0/0/1
D       172.31.7.12/30 [90/3193856] via 172.31.7.6, 00:00:07,
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.6, 00:00:11, Serial0/0/0
```

Rutas de nivel 1

Rutas de nivel 2

```
BOGOTA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 172.31.7.2 to network 0.0.0.0
172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D       172.31.0.0/24 [90/2684416] via 172.31.7.2, 00:17:33, Serial0/0/0
D       172.31.1.0/24 [90/2684416] via 172.31.7.2, 00:17:33, Serial0/0/0
D       172.31.2.0/23 [90/2172416] via 172.31.7.13, 00:38:27, Serial0/0/1
D       172.31.4.0/23 [90/2172416] via 172.31.7.13, 00:38:27, Serial0/0/1
C       172.31.7.0/30 is directly connected, Serial0/0/0
D       172.31.7.4/30 [90/2681856] via 172.31.7.2, 00:17:33,
D       172.31.7.8/30 [90/41024000] via 172.31.7.13, 00:38:2
C       172.31.7.12/30 is directly connected, Serial0/0/1
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.2, 00:17:33, Serial0/0/0
```

Rutas de nivel 1

Rutas de nivel 2

```
LIMA#sh ip route
……..<resultado omitido>……
Gateway of last resort is 172.31.7.14 to network 0.0.0.0
172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D       172.31.0.0/24 [90/3196416] via 172.31.7.14, 00:24:53, Serial0/0/0
D       172.31.1.0/24 [90/3196416] via 172.31.7.14, 00:24:53, Serial0/0/0
C       172.31.2.0/23 is directly connected, FastEthernet0/0
C       172.31.4.0/23 is directly connected, FastEthernet0/1
D       172.31.7.0/30 [90/2681856] via 172.31.7.14, 00:45:47
D       172.31.7.4/30 [90/3193856] via 172.31.7.14, 00:24:53
C       172.31.7.8/30 is directly connected, Serial0/0/1
C       172.31.7.12/30 is directly connected, Serial0/0/0
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.14, 00:24:53, Serial0/0/0
```

Rutas de nivel 1

Rutas de nivel 2

FASE II:

1. Se agrega el router Santiago, considerando sus cuatro subredes de 60 Hosts.
   - Para el caso se crean interfaces loopback y se establecen las subredes.
   - Asimismo, se requiere de una dirección para el enlace, punto a punto con el router Lima en la interfaz serial 0/0/0.
   - Finalmente se agrega la ruta estática hacia la red 172.31.0.0 /20 mediante la interfaz serial 0/0/0, ya que el router no participa del enrutamiento EIGRP.
   - Podría habilitarse una ruta por defecto para que se tenga alcance a Internet pero el caso no lo requiere. Adicionalmente a ello se necesitaría una ruta estática en el ISP que permita alcanzar la red de Santiago.

```
SANTIAGO#show running-config
Building configuration...
……..<resultado omitido>…….
hostname SANTIAGO
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.192
!
interface Loopback1
 ip address 192.168.2.65 255.255.255.192
!
interface Loopback2
 ip address 192.168.2.129 255.255.255.192
!
interface Loopback3
 ip address 192.168.2.193 255.255.255.192
!
interface Serial0/0/0
 ip address 199.1.1.2 255.255.255.252
 clock rate 64000
!
ip route 172.31.0.0 255.255.240.0 Serial0/0/0
!
……..<resultado omitido>…….
```

   - El router Lima deberá agregar, por lo tanto, una ruta estática que permita el acceso hacia las subredes del router Santiago. Esto se podría realizar de forma individual pero, para simplificar la configuración, se sumarizará en la dirección 192.168.2.0 /24.

```
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config-)# ip route 192.168.2.0 255.255.255.0 Serial0/1/0
LIMA(config)#router eigrp 65300
LIMA(config-router)#redi stribute static
```

   - Verificamos en el router Brasilia la tabla de enrutamiento y observamos que el sistema etiqueta esta nueva red como ruta externa (D EX), ya que es una ruta redistribuida.
   - Obsérvese que la ruta externa tiene una distancia administrativa de 170.

- Para el router, la red presenta una ruta de respaldo.

```
BRASILIA#sh ip route
……..<resultado omitido>…….

D EX 192.168.2.0/24 [170/3705856] via 172.31.7.6, 00:06:56, Serial0/0/0
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.6, 00:48:02, Serial0/0/0

BRASILIA#sh ip eigrp topology
IP-EIGRP Topology Table for AS 65300
……..<resultado omitido>…….

P 192.168.2.0/24, 1 successors, FD is 3705856
      via 172.31.7.6 (3705856/3193856), Serial0/0/0
      via 172.31.7.10 (4294967295/2169856), Serial0/0/1← Successor factible
```

2. Se configuran en el router Bogotá ocho subredes con 200 Hosts para cada una, con cuyo fin se definieron las subredes a partir de la dirección 172.20.0.0 como sigue:

```
BOGOTÁ#sh run
! ……..<resultado omitido>…….
interface Loopback0
 ip address 172.20.0.1 255.255.255.0
!
interface Loopback1
 ip address 172.20.1.1 255.255.255.0
!
interface Loopback2
 ip address 172.20.2.1 255.255.255.0
!
interface Loopback3
 ip address 172.20.3.1 255.255.255.0
!
interface Loopback4
 ip address 172.20.4.1 255.255.255.0
!
interface Loopback5
 ip address 172.20.5.1 255.255.255.0
!
interface Loopback6
 ip address 172.20.6.1 255.255.255.0
!
interface Loopback7
 ip address 172.20.7.1 255.255.255.0
!
……..<resultado omitido>…….
```

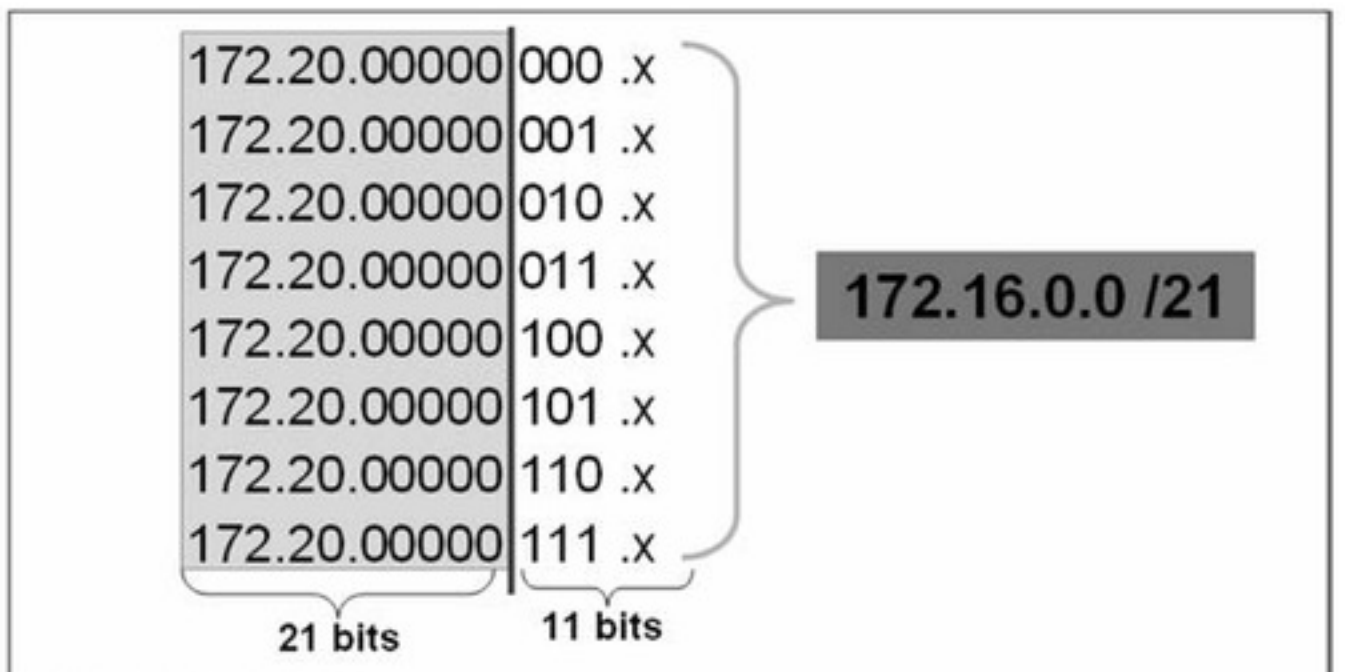
- Posteriormente se publica cada una de ellas dentro del enrutamiento EIGRP 65300.

```
BOGOTÁ(config)#router eigrp 65300
BOGOTÁ(config-router)#net 172.20.0.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.1.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.2.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.3.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.4.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.5.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.6.0 0.0.0.255
BOGOTÁ(config-router)#net 172.20.7.0 0.0.0.255
```

- Verificamos que aparecen las redes tal cual se publicaron, pero la tabla incrementa su tamaño, por lo que se recomienda una sumarización manual.

```
MIAMI#sh ip route eigrp
D      172.20.0.0/24 [90/2297856] via 172.31.7.1, 00:04:03, Serial0/0/0
D      172.20.1.0/24 [90/2297856] via 172.31.7.1, 00:03:58, Serial0/0/0
D      172.20.2.0/24 [90/2297856] via 172.31.7.1, 00:03:53, Serial0/0/0
D      172.20.3.0/24 [90/2297856] via 172.31.7.1, 00:03:44, Serial0/0/0
D      172.20.4.0/24 [90/2297856] via 172.31.7.1, 00:03:39, Serial0/0/0
D      172.20.5.0/24 [90/2297856] via 172.31.7.1, 00:03:35, Serial0/0/0
D      172.20.6.0/24 [90/2297856] via 172.31.7.1, 00:03:31, Serial0/0/0
D      172.20.7.0/24 [90/2297856] via 172.31.7.1, 00:03:27, Serial0/0/0
D      172.31.0.0/24 [90/2172416] via 172.31.7.5, 01:36:23, Serial0/1/0
D      172.31.1.0/24 [90/2172416] via 172.31.7.5, 01:36:23, Serial0/1/0
D      172.31.2.0/23 [90/2684416] via 172.31.7.1, 00:08:43, Serial0/0/0
D      172.31.4.0/23 [90/2684416] via 172.31.7.1, 00:08:43, Serial0/0/0
D      172.31.7.8/30 [90/41024000] via 172.31.7.5, 01:36:23, Serial0/1/0
D      172.31.7.12/30 [90/2681856] via 172.31.7.1, 00:08:44, Serial0/0/0
D EX 192.168.2.0/24 [170/3193856] via 172.31.7.1, 00:08:43, Serial0/0/0
```

- Manualmente se sumariza, lo cual da como resultado la dirección 172.20.0.0 /21, ya que sólo es necesario comparar el tercer octeto, arrojando una igualdad.



MASCARA DE SUBRED:
Como el resultado obtenido es hasta el BIT 21 la mascara será con 21 bits = 255.255.248.0

DIRECCION DE RESUMEN:
Los bits que resulten iguales se convierten a su equivalente decimal y se completa con ceros hasta el bit 32, lo cual resulta 172.16.0.0

- Habilitamos la sumarización manual en cada interfaz del router Bogotá, como se muestra:
- El comando de configuración del router eigrp log-neighbor-changes se encuentra activado de manera predeterminada en algunas implementaciones IOS. Si se encuentra activado, verá un resultado similar al mostrado para el router Bogotá.
- DUAL desactiva todas las adyacencias de vecinos y luego las reestablece para que el efecto del comando **ip summary-address eigrp** se logre en su totalidad. Todos los vecinos EIGRP enviarán inmediatamente una nueva serie de actualizaciones.

```
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#ip summary-address eigrp 65300 172.20.0.0 255.255.248.0
BOGOTA(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 65300: Neighbor 172.31.7.13 (Serial0/0/1) is up: new adjacency
BOGOTA(config-if)#int s0/0/1
BOGOTA(config-if)#ip summary-address eigrp 65300 172.20.0.0 255.255.248.0
%DUAL-5-NBRCHANGE: IP-EIGRP 65300: Neighbor 172.31.7.2 (Serial0/0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 65300: Neighbor 172.31.7.13 (Serial0/0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 65300: Neighbor 172.31.7.2 (Serial0/0/0) is up: new adjacency
```

- Verificamos luego la tabla de enrutamiento en los routers, observando una tabla más pequeña y sin etiqueta de ruta externa.
- El algoritmo DUAL identifica el resumen y sólo comenzará a publicar eliminando las entradas anteriores.

```
BOGOTA#sh ip route
Gateway of last resort is 172.31.7.2 to network 0.0.0.0
    172.20.0.0/16 is variably subnetted, 9 subnets, 2 masks
D      172.20.0.0/21 is a summary, 00:30:22, Null0
C      172.20.0.0/24 is directly connected, Loopback0
C      172.20.1.0/24 is directly connected, Loopback1
C      172.20.2.0/24 is directly connected, Loopback2
C      172.20.3.0/24 is directly connected, Loopback3
C      172.20.4.0/24 is directly connected, Loopback4
C      172.20.5.0/24 is directly connected, Loopback5
C      172.20.6.0/24 is directly connected, Loopback6
C      172.20.7.0/24 is directly connected, Loopback7
    172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D      172.31.0.0/24 [90/2684416] via 172.31.7.2, 00:30:17, Serial0/0/0
D      172.31.1.0/24 [90/2684416] via 172.31.7.2, 00:30:17, Serial0/0/0
D      172.31.2.0/23 [90/2172416] via 172.31.7.13, 00:30:20, Serial0/0/1
D      172.31.4.0/23 [90/2172416] via 172.31.7.13, 00:30:20, Serial0/0/1
C      172.31.7.0/30 is directly connected, Serial0/0/0
D      172.31.7.4/30 [90/2681856] via 172.31.7.2, 00:30:17, Serial0/0/0
D      172.31.7.8/30 [90/41024000] via 172.31.7.13, 00:30:20, Serial0/0/1
C      172.31.7.12/30 is directly connected, Serial0/0/1
D EX 192.168.2.0/24 [170/2681856] via 172.31.7.13, 00:30:20, Serial0/0/1
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.2, 00:30:17, Serial0/0/0
```

```
LIMA#sh ip route
Gateway of last resort is 172.31.7.14 to network 0.0.0.0
    172.20.0.0/21 is subnetted, 1 subnets
D      172.20.0.0 [90/2681856] via 172.31.7.14, 00:29:47, Serial0/0/0
    172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D      172.31.0.0/24 [90/3196416] via 172.31.7.14, 00:29:43, Serial0/0/0
D      172.31.1.0/24 [90/3196416] via 172.31.7.14, 00:29:43, Serial0/0/0
C      172.31.2.0/23 is directly connected, FastEthernet0/0
C      172.31.4.0/23 is directly connected, FastEthernet0/1
D      172.31.7.0/30 [90/2681856] via 172.31.7.14, 00:29:47, Serial0/0/0
D      172.31.7.4/30 [90/3193856] via 172.31.7.14, 00:29:43, Serial0/0/0
C      172.31.7.8/30 is directly connected, Serial0/0/1
C      172.31.7.12/30 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/1/0
    199.1.1.0/30 is subnetted, 1 subnets
C      199.1.1.0 is directly connected, Serial0/1/0
D*EX 0.0.0.0/0 [170/3193856] via 172.31.7.14, 00:29:43, Serial0/0/0
```

```
MIAMI#sh ip route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.20.0.0/21 is subnetted, 1 subnets
D      172.20.0.0 [90/2681856] via 172.31.7.1, 00:30:55, Serial0/0/0
    172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
D      172.31.0.0/24 [90/2172416] via 172.31.7.5, 02:15:23, Serial0/1/0
D      172.31.1.0/24 [90/2172416] via 172.31.7.5, 02:15:23, Serial0/1/0
D      172.31.2.0/23 [90/2684416] via 172.31.7.1, 00:30:55, Serial0/0/0
D      172.31.4.0/23 [90/2684416] via 172.31.7.1, 00:30:55, Serial0/0/0
C      172.31.7.0/30 is directly connected, Serial0/0/0
C      172.31.7.4/30 is directly connected, Serial0/1/0
D      172.31.7.8/30 [90/41024000] via 172.31.7.5, 02:15:23, Serial0/1/0
D      172.31.7.12/30 [90/2681856] via 172.31.7.1, 00:30:55, Serial0/0/0
D EX 192.168.2.0/24 [170/3193856] via 172.31.7.1, 00:30:55, Serial0/0/0
C    200.1.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

```
BRASILIA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
Gateway of last resort is 172.31.7.6 to network 0.0.0.0
    172.20.0.0/21 is subnetted, 1 subnets
D      172.20.0.0 [90/3193856] via 172.31.7.6, 00:31:32, Serial0/0/0
    172.31.0.0/16 is variably subnetted, 8 subnets, 3 masks
C      172.31.0.0/24 is directly connected, FastEthernet0/0
C      172.31.1.0/24 is directly connected, FastEthernet0/1
D      172.31.2.0/23 [90/3196416] via 172.31.7.6, 00:31:32, Serial0/0/0
D      172.31.4.0/23 [90/3196416] via 172.31.7.6, 00:31:32, Serial0/0/0
D      172.31.7.0/30 [90/2681856] via 172.31.7.6, 02:16:00, Serial0/0/0
C      172.31.7.4/30 is directly connected, Serial0/0/0
C      172.31.7.8/30 is directly connected, Serial0/0/1
D      172.31.7.12/30 [90/3193856] via 172.31.7.6, 00:31:32, Serial0/0/0
D EX 192.168.2.0/24 [170/3705856] via 172.31.7.6, 00:31:32, Serial0/0/0
D*EX 0.0.0.0/0 [170/2681856] via 172.31.7.6, 02:16:00, Serial0/0/0
```

FASE III

- Capture la información de cada router:
  a. Tabla de vecinos.
  b. Tabla de topología.
  c. Tabla de enrutamiento.
  d. Configuración activa.

OBSERVACIONES Y/O COMENTARIOS

LABORATORIO N° 10 - OSPF

DESCRIPCIÓN

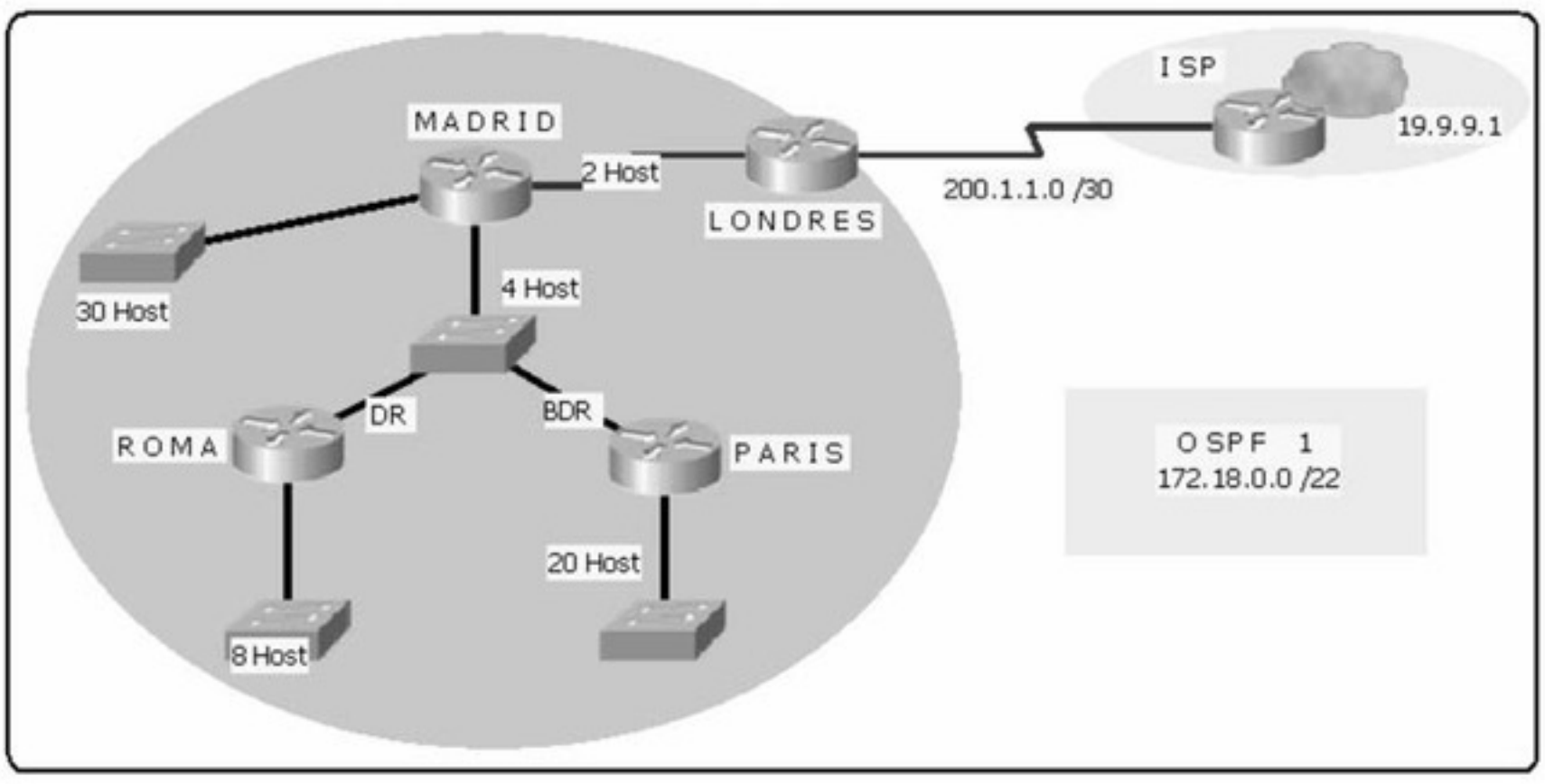
Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace similar a IS-IS, desarrollado para reemplazar a RIP. Entre sus principales ventajas están su rápida convergencia y escalabilidad a implementaciones de redes muchos mayores. Emplea el ancho de banda como la métrica de costo.

OBJETIVOS

- Configuración del enrutamiento mediante el protocolo OSPF en una sola área.
- Redistribución de ruta por defecto dentro del proceso OSPF.
- Optimizar el enrutamiento OSPF dentro de un área, para una red multiacceso con broadcast.

PLANTEAMIENTO

Se presenta el esquema de red con los requerimientos de Host y su conexión de salida a Internet mediante el enrutamiento OSPF en área 0.



Se requiere de:

- Enrutamiento OSPF en el área 0.
- Ruta por defecto hacia la conexión ISP (Internet).
- Redistribución de la ruta por defecto dentro del área 0.
- Definir el router Roma como DR y el router París, como BDR.
- Modifique los intervalos de tiempo para un proceso de intercambio más lento.

DESARROLLO

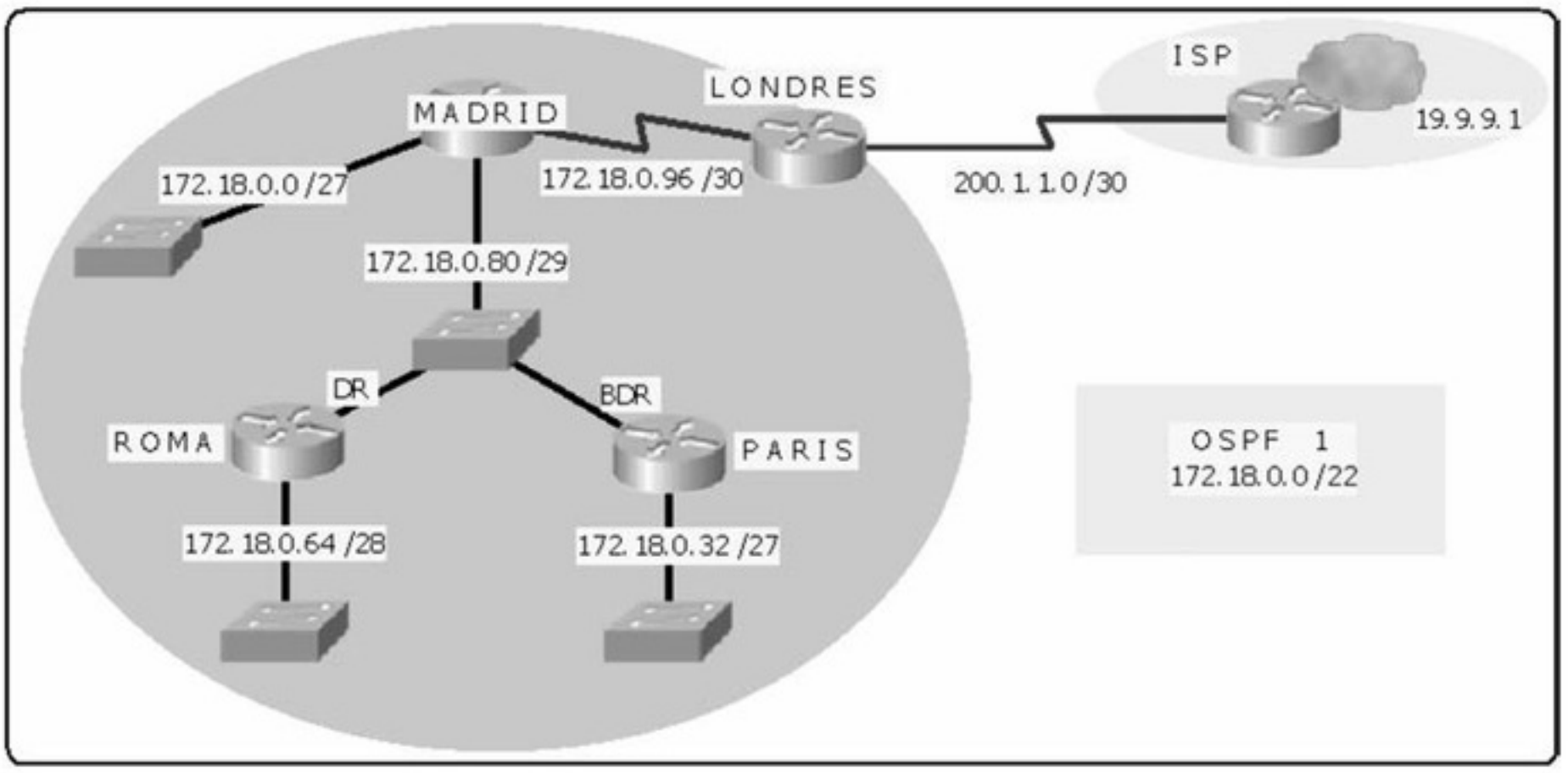
Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

FASE I: PASOS PREVIOS:

1. Realice las conexiones y elimine la configuración de cada router, en caso la tenga.
2. Habilite la opción de captura de texto en el Hyperterminal.
3. Realice la configuración básica con ayuda del editor de texto.

FASE II DIRECCIONAMIENTO Y CONFIGURACIÓN:

1. **DIRECCIONAMIENTO IP**
   - El direccionamiento se muestra de acuerdo a los requerimientos de Host en las respectivas ubicaciones.



2. **Direcciones loopback**:
   - En una dirección loopback se debe siempre tener en cuenta el uso de la interfaz, ya que permite mantener activo el proceso OSPF además de ser una interfaz virtual y no física, por lo que no se verá afectada por un problema de capa 1.
   - Considerar el ID del router para la elección del DR y BDR. Para el caso, el router Roma presenta la dirección más alta.
     - Roma: Loopback 0 = 199.22.22.22.1 /32
     - París: Loopback 0 = 199.20.20.1 /32
     - Madrid: Loopback 0 = 199.19.19.19.1 /32
     - Londres: Loopback 0 = 199.9.9.1 /32

3. **Enrutamiento OSPF y ruta por defecto**

- Al router Londres se le denomina, en ocasiones, router de borde, entrada o gateway. Sin embargo, en la terminología OSPF, se le conoce como el ASBR (*Autonomous System Boundary Router*).
- El comando default-information originate publicará la ruta por defecto a los demás routers del área.

```
router ospf 1
 log-adjacency-changes
 network 172.18.0.96 0.0.0.3 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
……..< resultado omitido >…….
```

- El enrutamiento OSPF se habilita dentro del área 0, manejando las direcciones wildcard-mask de acuerdo a la subred.

```
MADRID(config)#router ospf 1
MADRID(config-router)#net 172.18.0.0 0.0.0.31 area 0
MADRID(config-router)#net 172.18.0.96 0.0.0.3 area 0
MADRID(config-router)#net 172.18.0.80 0.0.0.7 area 0
00:49:40: %OSPF-5-ADJCHG: Process 1, Nbr 199.9.9.1 on Serial0/0/0 from LOADING to FULL, Loading
Done
00:49:51: %OSPF-5-ADJCHG: Process 1, Nbr 199.22.22.1 on FastEthernet0/0 from EXCHANGE to FULL,
Exchange Done
00:49:53: %OSPF-5-ADJCHG: Process 1, Nbr 199.20.20.1 on FastEthernet0/0 from EXCHANGE to FULL,
Exchange Done
MADRID(config-router)#
```

4. **TABLA DE VECINOS**

- El ID de un router es una dirección IP. Considerando la siguiente prioridad: 1. dirección IP configurada con el comando **router-id**; 2. la dirección IP más alta de cualquiera de sus interfaces loopback; 3. la dirección IP activa más alta de cualquiera de sus interfaces físicas.
- A continuación podemos identificar el ID en el router con el comando **show ip protocols**.

```
MADRID#show ip protocols
Routing Protocol is “ospf 1”
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 199.19.19.1    ←---------- ID en el router
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa

……..< resultado omitido >…….
```

- Es conveniente verificar el ID del router ya que sino podría asumirse otra dirección de cualquier interfaz.
- De acuerdo con el intercambio de saludo inicial dentro del área definida, se identifican los vecinos y cada router se identifica con su ID respectivo.

```
LONDRES#SH IP OSPF NEighbor
Neighbor ID    Pri   State          Dead Time   Address        Interface
199.19.19.1      1   FULL/-         00:00:33    172.18.0.97    Serial0/0/0
```

```
MADRID#SH IP OSPF NEighbor
Neighbor ID    Pri   State          Dead Time   Address        Interface
199.20.20.1      1   FULL/BDR       00:00:38    172.18.0.82    FastEthernet0/0
199.22.22.1      1   FULL/DR        00:00:38    172.18.0.81    FastEthernet0/0
199.9.9.1        1   FULL/-         00:00:35    172.18.0.98    Serial0/0/0
```

```
ROMA#SH IP OSPF NEighbor
Neighbor ID    Pri   State          Dead Time   Address        Interface
199.20.20.1      1   FULL/BDR       00:00:30    172.18.0.82    FastEthernet0/0
199.19.19.1      1   FULL/DROTHER   00:00:35    172.18.0.83    FastEthernet0/0
```

```
PARÍS#show ip ospf neighbor
Neighbor ID    Pri   State          Dead Time   Address        Interface
199.22.22.1      1   FULL/DR        00:00:30    172.18.0.81    FastEthernet0/0
199.19.19.1      1   FULL/DROTHER   00:00:35    172.18.0.83    FastEthernet0/0
```

5. BASE DE DATOS TOPOLÓGICA

- La información que los routers intercambian se basa en las redes declaradas para el enrutamiento.
- Así, el router PARÍS publicará las redes 172.18.0.80 y 172.18.0.32 dentro del área 0.

```
PARÍS#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 199.20.20.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.18.0.80 0.0.0.7 area 0
    172.18.0.32 0.0.0.31 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.18.0.81          110      00:12:21
    172.18.0.83          110      00:12:21
  Distance: (default is 110)
```

- La base de datos topológica mostrará el listado de vecinos en toda el área 0, así como rutas tipo 5 que son consideradas por ser enlaces externos, como la ruta por defecto que tiene el router Londres, y los redistribuye en el área 0.

```
LONDRES#SH IP OSPF DAtabase
        OSPF Router with ID (199.9.9.1) (Process ID 1)
          Router Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum Link count
199.9.9.1       199.9.9.1      622       0x80000009 0x00feff 2
199.20.20.1   199.20.20.1    640       0x80000004 0x00feff 2
199.22.22.1   199.22.22.1    639       0x80000004 0x00feff 2
199.19.19.1   199.19.19.1    575       0x80000008 0x00feff 4
          Net Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum
172.18.0.81   199.22.22.1    575       0x80000003 0x004a83
          Type-5 AS External Link States
Link ID       ADV Router     Age       Seq#      Checksum Tag
0.0.0.0       199.9.9.1      679       0x80000002 0x00feff 1
LONDRES#
```

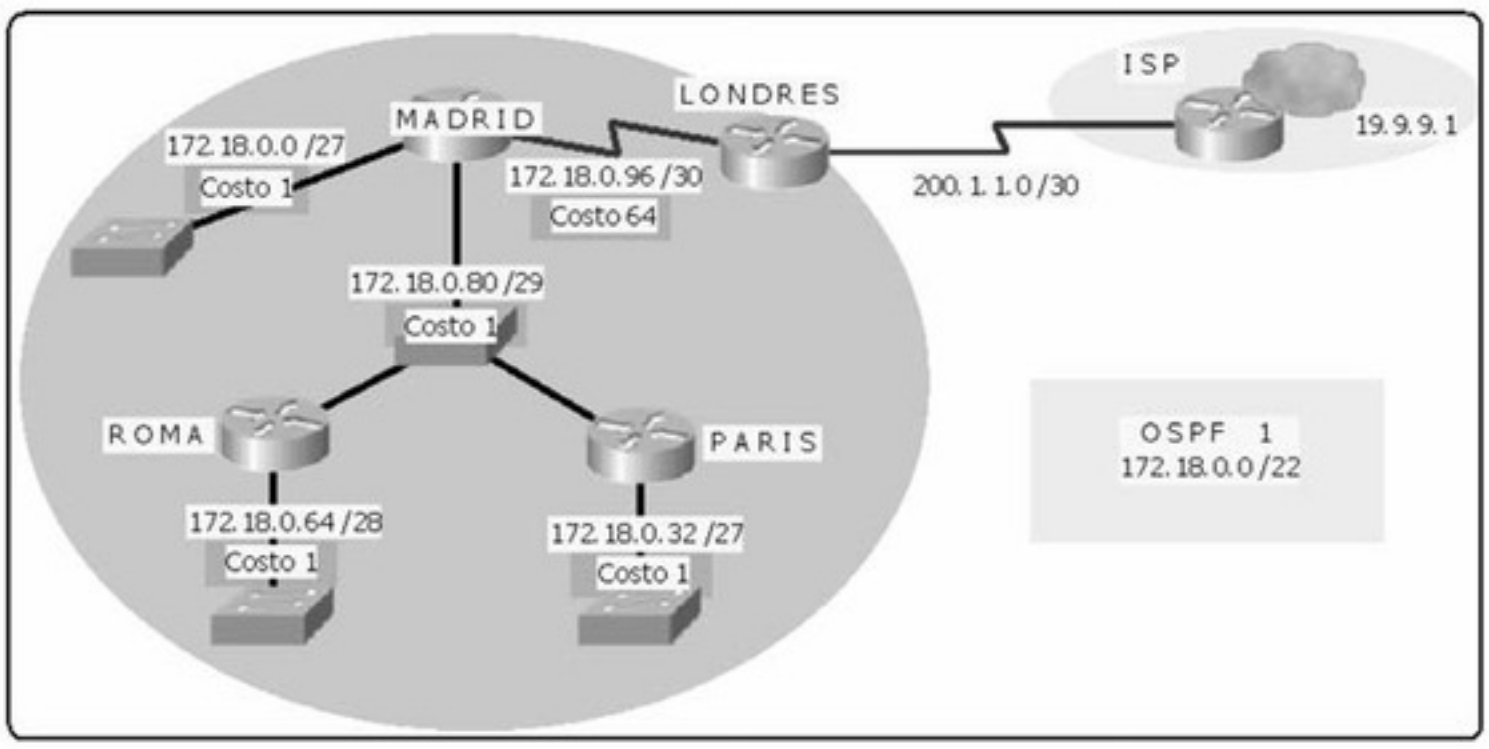
```
MADRID#SH IP OSPF DATAbase
        OSPF Router with ID (199.19.19.1) (Process ID 1)
          Router Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum Link count
199.19.19.1   199.19.19.1    468       0x80000008 0x00feff 4
199.20.20.1   199.20.20.1    533       0x80000004 0x00feff 2
199.22.22.1   199.22.22.1    533       0x80000004 0x00feff 2
199.9.9.1       199.9.9.1      516       0x80000009 0x00feff 2
          Net Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum
172.18.0.81   199.22.22.1    469       0x80000003 0x004a83
          Type-5 AS External Link States
Link ID       ADV Router     Age       Seq#      Checksum Tag
0.0.0.0       199.9.9.1      573       0x80000002 0x00feff 1
```

```
ROMA#SH IP OSPF DATABASE
        OSPF Router with ID (199.22.22.1) (Process ID 1)
          Router Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum Link count
199.22.22.1   199.22.22.1    815       0x80000004 0x00feff 2
199.20.20.1   199.20.20.1    816       0x80000004 0x00feff 2
199.9.9.1       199.9.9.1      799       0x80000009 0x00feff 2
199.19.19.1   199.19.19.1    751       0x80000008 0x00feff 4
          Net Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum
172.18.0.81   199.22.22.1    751       0x80000003 0x004a83
          Type-5 AS External Link States
Link ID       ADV Router     Age       Seq#      Checksum Tag
0.0.0.0       199.9.9.1      856       0x80000002 0x00feff 1
```

```
PARÍS#show ip ospf database
        OSPF Router with ID (199.20.20.1) (Process ID 1)
            Router Link States (Area 0)
Link ID      ADV Router     Age      Seq#       Checksum Link count
199.20.20.1  199.20.20.1    948      0x80000004 0x00feff 2
199.22.22.1  199.22.22.1    948      0x80000004 0x00feff 2
199.9.9.1    199.9.9.1      931      0x80000009 0x00feff 2
199.19.19.1  199.19.19.1    884      0x80000008 0x00feff 4
            Net Link States (Area 0)
Link ID      ADV Router     Age      Seq#       Checksum
172.18.0.81  199.22.22.1    884      0x80000003 0x004a83
            Type-5 AS External Link States
Link ID      ADV Router     Age      Seq#       Checksum Tag
0.0.0.0      199.9.9.1      988      0x80000002 0x00feff 1
```

6. **ANÁLISIS DEL COSTO Y LA TABLA DE ENRUTAMIENTO:**

- OSPF acumula costos. El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino. El valor del ancho de banda de cada interfaz se calcula con 100 000 000/ancho de banda.
- A continuación se muestra el diagrama de red con el costo de cada enlace para su comparación hacia cada una de las rutas:



- La tabla de enrutamiento resume cada una de las redes identificadas por OSPF junto a su métrica, dentro del área 0. Nótese, asimismo, que la ruta por defecto se etiqueta como O*E2.

```
LONDRES#SH IP ROU
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.18.0.0/16 is variably subnetted, 5 subnets, 4 masks
O      172.18.0.0/27 [110/65] via 172.18.0.97, 00:40:53, Serial0/0/0
O      172.18.0.32/27 [110/66] via 172.18.0.97, 00:39:56, Serial0/0/0
O      172.18.0.64/28 [110/66] via 172.18.0.97, 00:39:56, Serial0/0/0
O      172.18.0.80/29 [110/65] via 172.18.0.97, 00:39:56, Serial0/0/0
C      172.18.0.96/30 is directly connected, Serial0/0/0
    199.9.9.0/32 is subnetted, 1 subnets
C      199.9.9.1 is directly connected, Loopback0
    200.1.1.0/30 is subnetted, 1 subnets
C      200.1.1.0 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

```
MADRID#SH IP ROUTE
Gateway of last resort is 172.18.0.98 to network 0.0.0.0
    172.18.0.0/16 is variably subnetted, 5 subnets, 4 masks
C       172.18.0.0/27 is directly connected, FastEthernet0/1
O       172.18.0.32/27 [110/2] via 172.18.0.82, 00:35:43, FastEthernet0/0
O       172.18.0.64/28 [110/2] via 172.18.0.81, 00:35:43, FastEthernet0/0
C       172.18.0.80/29 is directly connected, FastEthernet0/0
C       172.18.0.96/30 is directly connected, Serial0/0/0
    199.19.19.0/32 is subnetted, 1 subnets
C       199.19.19.1 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 172.18.0.98, 00:36:26, Serial0/0/0
```

```
ROMA#show ip route
Gateway of last resort is 172.18.0.83 to network 0.0.0.0
    172.18.0.0/16 is variably subnetted, 5 subnets, 4 masks
O       172.18.0.0/27 [110/2] via 172.18.0.83, 00:43:15, FastEthernet0/0
O       172.18.0.32/27 [110/2] via 172.18.0.82, 00:44:20, FastEthernet0/0
C       172.18.0.64/28 is directly connected, FastEthernet0/1
C       172.18.0.80/29 is directly connected, FastEthernet0/0
O       172.18.0.96/30 [110/65] via 172.18.0.83, 00:43:15, FastEthernet0/0
    199.22.22.0/32 is subnetted, 1 subnets
C       199.22.22.1 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 172.18.0.83, 00:43:15, FastEthernet0/0
```

```
PARÍS#show ip route
Gateway of last resort is 172.18.0.83 to network 0.0.0.0
    172.18.0.0/16 is variably subnetted, 5 subnets, 4 masks
O       172.18.0.0/27 [110/2] via 172.18.0.83, 00:46:13, FastEthernet0/0
C       172.18.0.32/27 is directly connected, FastEthernet0/1
O       172.18.0.64/28 [110/2] via 172.18.0.81, 00:47:18, FastEthernet0/0
C       172.18.0.80/29 is directly connected, FastEthernet0/0
O       172.18.0.96/30 [110/65] via 172.18.0.83, 00:46:13, FastEthernet0/0
    199.20.20.0/32 is subnetted, 1 subnets
C       199.20.20.1 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 172.18.0.83, 00:46:13, FastEthernet0/0
```

La etiqueta O*E2 denota que ésta es una ruta OSPF externa tipo 2. Las rutas OSPF externas se encuentran en una de las dos siguientes categorías: External Type 1 (Externa Tipo 1, E1) o External Type 2 (Externa Tipo 2, E2). El costo de una ruta E2 es siempre el costo externo, independientemente del costo interior para alcanzar dicha ruta.

FASE III OPTIMIZANDO LA RED

1. **DEFINICIÓN DEL DR Y BDR**
   - El requerimiento del esquema inicial exige la elección del router Roma como DR y el router París, como BDR. Con ayuda del ID de cada router, sobre la base de la dirección loopback, se logró inicialmente ello pero no es del todo segura dicha opción.
   - Para elegir el router DR y BDR, se recomienda controlar la elección con el comando **ip ospf priority interface**, para un mejor control de las redes. También se permite a un a router ser DR en una red y DROther, en otra.

- Para el caso se han modificado las prioridades de los routers:
- El router Roma, con prioridad 255.
- El router París, con prioridad 250.
- El router Madrid tiene prioridad 0 (no participa).
- Después de ejecutar, deshabilitar y habilitar las interfaces FastEthernet 0/0 de los tres routers (realizarlo al mismo tiempo), también puede ejecutar el comando **clear ip ospf process**.
- A continuación vemos el resultado del cambio de las prioridades.

```
MADRID#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
199.22.22.1     255   FULL/DR         00:00:38    172.18.0.81     FastEthernet0/0
199.20.20.1     250   FULL/BDR        00:00:34    172.18.0.82     FastEthernet0/0
199.9.9.1         1   FULL/-          00:00:37    172.18.0.98     Serial0/0/0
```

```
PARÍS#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
199.22.22.1     255   FULL/DR         00:00:34    172.18.0.81     FastEthernet0/0
199.19.19.1       0   FULL/DROTHER    00:00:34    172.18.0.83     FastEthernet0/0
```

```
ROMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
199.19.19.1       0   FULL/DROTHER    00:00:32    172.18.0.83     FastEthernet0/0
199.20.20.1     250   FULL/BDR        00:00:38    172.18.0.82     FastEthernet0/0
```

- En resumen, esta es la información que se presenta en la topología:

Router	ID del router	Prioridad	Estado
ROMA	199.22.22.1	255	DR
PARÍS	199.20.20.1	250	BDR
MADRID	199.19.19.1	0	DROTHER

FASE IV TEMPORIZADORES

- Puede ser aconsejable cambiar los temporizadores OSPF para que los routers detecten las fallas de red en menor tiempo. Si bien al hacerlo se aumentará el tráfico, en ocasiones se necesita una convergencia rápida que compense el tráfico adicional.

***Nota**: OSPF requiere que los intervalos muerto y de saludo coincidan entre dos routers para que sean adyacentes. Esto es distinto de EIGRP donde los temporizadores de saludo y de espera no necesitan coincidir para que dos routers formen una adyacencia EIGRP.*

- Modificamos los intervalos de tiempo en la interfaz serial 0/0/0 del router Madrid y observamos que por este motivo se pierde adyacencia con el router de ID (Londres).
- Al observar, la tabla de vecinos ya no figura en el listado.

```
MADRID(config)#INT S0/0/0
MADRID(config-if)#IP OSPF Hello-interval 20
MADRID(config-if)#IP OSPF Dead-interval 80
MADRID(config-if)#
03:58:54: %OSPF-5-ADJCHG: Process 1, Nbr 199.9.9.1 on Serial0/0/0 from FULL to DOWN, Neighbor
Down: Dead timer expired
03:58:54: %OSPF-5-ADJCHG: Process 1, Nbr 199.9.9.1 on Serial0/0/0 from FULL to Down: Interface
down or detached
MADRID(config-if)#

MADRID#sh ip ospf neighbor
Neighbor ID    Pri   State         Dead Time   Address       Interface
199.22.22.1    255   FULL/DR       00:00:34    172.18.0.81    FastEthernet0/0
199.20.20.1    250   FULL/BDR      00:00:31    172.18.0.82    FastEthernet0/0
MADRID#
```

- Observando posteriormente, notaremos que el router Londres muestra un mensaje de desactivación respecto a la adyacencia con el router de ID 199.19.19.1 (Madrid) en su interfaz serial 0/0/0. Al revisar, la tabla de vecinos se muestra en blanco.

```
LONDRES#09:22:45: %OSPF-5-ADJCHG: Process 1, Nbr 199.19.19.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired!
end
09:22:45: %OSPF-5-ADJCHG: Process 1, Nbr 199.19.19.1 on Serial0/0/0 from FULL to Down: Interface
down or detached
LONDRES#sh ip ospf neighbor
LONDRES#
```

- Posteriormente modificamos los intervalos en la interfase serial 0/0/0 del router Londres, donde se muestra inmediatamente un mensaje de intercambio detectando la adyacencia con el router de ID 199.19.19.1 (Madrid) en estado FULL.
- La tabla de vecinos nuevamente muestra la adyacencia con el router de ID 199.19.19.1 (Madrid).

```
LONDRES#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LONDRES(config)#interface 0/0/0
LONDRES(config-if)#ip ospf hello-interval 20
LONDRES(config-if)#ip ospf dead-interval 80
LONDRES(config-if)#
09:32:21: %OSPF-5-ADJCHG: Process 1, Nbr 199.19.19.1 on Serial0/0/0 from EXCHANGE to FULL,
Exchange Done
LONDRES(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
LONDRES#sh ip ospf neighbor
Neighbor ID    Pri   State         Dead Time   Address       Interface
199.19.19.1     1    FULL/-        00:01:16    172.18.0.97    Serial0/0/0
LONDRES#
```

- En el router Madrid se observa un mensaje indicando que se estableció la adyacencia con un estado en FULL respecto al router con ID 199.9.9.1 (Londres); asimismo, se restablece la tabla de vecinos.

```
MADRID#
04:08:24: %OSPF-5-ADJCHG: Process 1, Nbr 199.9.9.1 on Serial0/0/0 from EXCHANGE to FULL, Exchange
Done
MADRID#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
199.22.22.1     255   FULL/DR         00:00:37    172.18.0.81     FastEthernet0/0
199.20.20.1     250   FULL/BDR        00:00:34    172.18.0.82     FastEthernet0/0
199.9.9.1         1   FULL/-          00:01:06    172.18.0.98     Serial0/0/0
MADRID#
```

CONFIGURACIÓN ACTIVA

```
LONDRES#sh running-config
Building configuration...
Current configuration : 1815 bytes
!
version 12.4
no service password-encryption
!
hostname LONDRES
!
interface Loopback0
 ip address 199.9.9.1 255.255.255.255
!
!
interface Serial0/0/0
 ip address 172.18.0.98 255.255.255.252
!
interface Serial0/0/1
 ip address 200.1.1.1 255.255.255.252
 clock rate 64000
!
router ospf 1
 log-adjacency-changes
 network 172.18.0.96 0.0.0.3 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
……..< resultado omitido >…….
```

```
MADRID#SH RUnning-config
Building configuration...
Current configuration : 1835 bytes
!
version 12.4
no service password-encryption
!
hostname MADRID
!
!
interface Loopback0
```

```
 ip address 199.19.19.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.18.0.83 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.18.0.1 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.18.0.97 255.255.255.252
 clock rate 64000
!
!
router ospf 1
 log-adjacency-changes
 network 172.18.0.80 0.0.0.7 area 0
 network 172.18.0.96 0.0.0.3 area 0
 network 172.18.0.0 0.0.0.31 area 0
!
……..< resultado omitido >…….
```

```
ROMA#show running-config
Building configuration...
Current configuration : 1766 bytes
!
version 12.4
no service password-encryption
!
hostname ROMA
!
!
interface Loopback0
 ip address 199.22.22.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.18.0.81 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.18.0.65 255.255.255.240
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 172.18.0.80 0.0.0.7 area 0
 network 172.18.0.64 0.0.0.15 area 0
!
……..< resultado omitido >…….
```

```
PARÍS#show running-config
Building configuration...
Current configuration : 1767 bytes
!
version 12.4
no service password-encryption
!
hostname PARÍS
!
!
interface Loopback0
 ip address 199.20.20.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.18.0.82 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.18.0.33 255.255.255.224
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 172.18.0.80 0.0.0.7 area 0
 network 172.18.0.32 0.0.0.31 area 0
!
……..< resultado omitido >…….
```

CONCLUSIONES Y/U OBSERVACIONES

_____

_____

_____

_____

Laboratorio N° 11 - OSPF - OPCIONES AVANZADAS

INTRODUCCIÓN

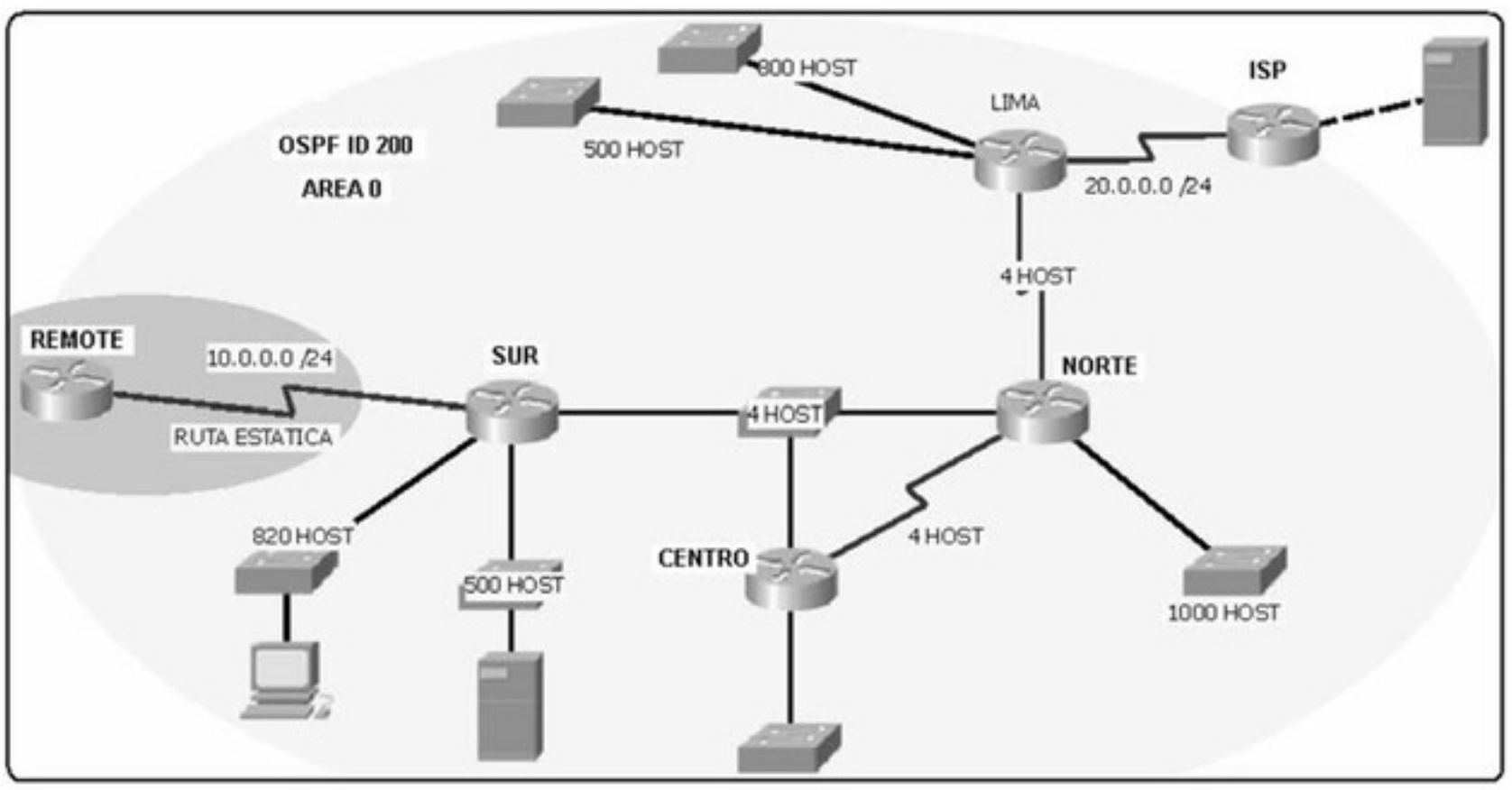
El protocolo OSPF (*Open Shortest Path First*) es uno de los más desarrollados como protocolo de enrutamiento interior para redes corporativas medianas y grandes.

OSPF es un protocolo apto para su implementación en redes de todo tipo y tamaño. Sin embargo, su debilidad principal es que demanda una configuración más compleja que otros protocolos, sobre todo para redes pequeñas.

OBJETIVOS

- Configurar el protocolo OSPF en forma básica y avanzada.

DESCRIPCIÓN

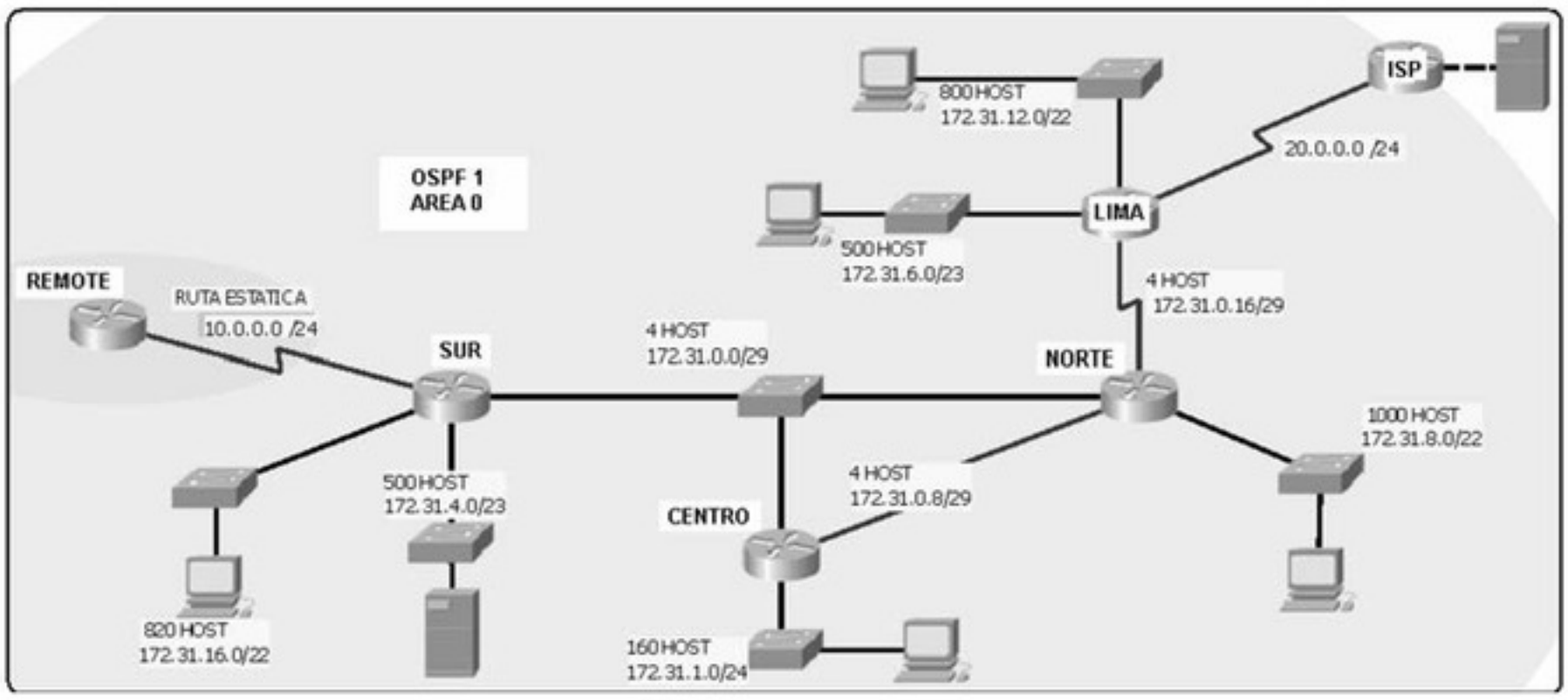


FASE I: CONFIGURACIÓN BÁSICA DE OSPF

1. Resolver el direccionamiento por VLSM mediante la dirección 172.31.0.0 /18.
2. Realizar la configuración básica de cada router.
3. Habilitar el enrutamiento según las características de la red.
4. Verificar las rutas internas y externas de OSPF.
5. Capturar la siguiente información:
   - Configuración activa.
   - Tabla de vecinos OSPF (indique los detalles de la información mostrada).
   - Tabla de enrutamiento (indique las rutas de nivel 1, 2, rutas principales y secundarias).
   - Características de las interfaces (indique los datos mencionados).

DESARROLLO DE FASE I:

1. Solución al problema de direccionamiento:



2. Habilitar el enrutamiento según las características de la red.

```
LIMA(config)#router ospf 1
LIMA(config-router)#net 172.31.6.0 0.0.3.255 area 0
LIMA(config-router)#net 172.31.12.0 0.0.3.255 area 0
LIMA(config-router)#no net 172.31.6.0 0.0.3.255 area 0
LIMA(config-router)#net 172.31.6.0 0.0.1.255 area 0
LIMA(config-router)#net 172.31.0.16 0.0.0.7 area 0
LIMA(config-router)#end
```

3. Verificamos rutas internas y externas de OSPF con la tabla de enrutamiento:
   - Como se observa, sólo existen rutas internas de OSPF ya que no se realizó ninguna redistribución de rutas ni tampoco existen otras áreas OSPF.

```
LIMA#sh ip route
Gateway of last resort is not set
     172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
O       172.31.0.0/29 [110/782] via 172.31.0.17, 00:00:06, Serial3/0
O       172.31.0.8/29 [110/1562] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.0.16/29 is directly connected, Serial3/0
O       172.31.1.0/24 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
O       172.31.4.0/23 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.6.0/23 is directly connected, FastEthernet0/0
O       172.31.8.0/22 [110/782] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.12.0/22 is directly connected, FastEthernet1/0
O       172.31.16.0/22 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
```

4. Configuración activa.
   - A manera de ejemplo se muestra la configuración completa del router Lima, que se tiene hasta después de habilitar el enrutamiento.

```
LIMA#sh ru
Building configuration...
Current configuration : 848 bytes
!
version 12.2
no service password-encryption
!
hostname LIMA
!
!
enable secret 5 $1$mERr$uOE542wOw.DoasRci5JOU0
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 172.31.6.1 255.255.254.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 172.31.12.1 255.255.252.0
 duplex auto
 speed auto
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 ip address 172.31.0.18 255.255.255.248
!
!
router ospf 1
 log-adjacency-changes
 network 172.31.12.0 0.0.3.255 area 0
 network 172.31.6.0 0.0.1.255 area 0
 network 172.31.0.16 0.0.0.7 area 0
!
ip classless
!
!
!
no cdp run
!
line con 0
 password lima
 login
line vty 0 4
 password lima
 login
!
!
end
```

5. **TABLA DE VECINOS**

- Para el caso del router Lima, el único vecino OSPF que tiene es el router Norte, identificado con el ID 172.31.8.1.
- En un enlace serial no existe DR ni BDR, por lo que el estado de la conexión sólo se menciona que está en FULL/.

```
LIMA#sh ip ospf nei
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.8.1        1   FULL/-          00:00:35    172.31.0.17     Serial3/0
```

- En los routers Norte, Centro y Sur deberá definirse el DR y BDR, ya que presentan una conexión FastEthernet en común.
- Para el caso, el router elegido es Centro, y el router Norte, el BDR.

```
NORTE#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.0.1        1   FULL/DROTHER    00:00:34    172.31.0.1      FastEthernet1/0
172.31.0.6        1   FULL/DR         00:00:34    172.31.0.6      FastEthernet1/0
172.31.12.1       0   FULL/ -         00:00:11    172.31.0.18     Serial2/0
172.31.0.6        0   FULL/ -         00:00:34    172.31.0.9      Serial3/0
```

- Adicionalmente a ello existe una conexión por interfaz serial entre los routers Norte y Centro donde, como ya se mencionó, no se elige un DR.

```
CENTRO#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.0.5        1   FULL/BDR        00:00:34    172.31.0.5      FastEthernet1/0
172.31.0.1        1   FULL/DROTHER    00:00:33    172.31.0.1      FastEthernet1/0
172.31.0.5        0   FULL/ -         00:00:39    172.31.0.10     Serial2/0
```

```
SUR#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.0.5        1   FULL/BDR        00:00:39    172.31.0.5      FastEthernet7/0
172.31.0.6        1   FULL/DR         00:00:39    172.31.0.6      FastEthernet7/0
```

6. **TABLA DE ENRUTAMIENTO**

- La tabla mostrada indica que las redes son de nivel 2 al ser parte de subredes y parten de una dirección general como lo es la dirección 172.31.0.0 /16.

```
LIMA#sh ip route
Gateway of last resort is not set
     172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
O       172.31.0.0/29 [110/782] via 172.31.0.17, 00:00:06, Serial3/0
O       172.31.0.8/29 [110/1562] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.0.16/29 is directly connected, Serial3/0
O       172.31.1.0/24 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
O       172.31.4.0/23 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.6.0/23 is directly connected, FastEthernet0/0
O       172.31.8.0/22 [110/782] via 172.31.0.17, 00:00:06, Serial3/0
C       172.31.12.0/22 is directly connected, FastEthernet1/0
O       172.31.16.0/22 [110/783] via 172.31.0.17, 00:00:06, Serial3/0
```

7. INTERFACES EN EL PROCESO OSPF

1. En este ejemplo tomaremos al router Norte, ya que tiene cuatro interfaces participando del proceso OSPF. El ID del router es 172.31.0.5.
2. La interfaz FastEthernet0/0 no presenta conexión hacia la topología de red OSPF directamente pero al estar mencionada en la publicación, el sistema define que será el DR para la red, donde se conecte, por ser el único, además.

```
NORTE#sh ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.31.8.1/22, Area 0
  Process ID 1, Router ID 172.31.0.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.31.0.5, Interface address 172.31.8.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

8. La interfaz FastEthernet1/0 está conectada a la red de los routers Centro y Sur, por lo que requiere obligatoriamente de un DR y BDR. Según el caso, se indica que ha sido definida como el BDR en esta red y que el DR es el router con el ID 172.31.0.6.

```
FastEthernet1/0 is up, line protocol is up
  Internet address is 172.31.0.5/29, Area 0
  Process ID 1, Router ID 172.31.0.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.31.0.6, Interface address 172.31.0.6
  Backup Designated Router (ID) 172.31.0.5, Interface address 172.31.0.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 172.31.0.1
    Adjacent with neighbor 172.31.0.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

9. Las interfaces seriales no requieren de un DR ya que el enlace es punto a punto, como se muestra.

```
Serial2/0 is up, line protocol is up
  Internet address is 172.31.0.17/29, Area 0
  Process ID 1, Router ID 172.31.0.5, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 4, Dead 15, Wait 15, Retransmit 5
    Hello due in 00:00:02
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.31.12.1
  Suppress hello for 0 neighbor(s)
```

```
Serial3/0 is up, line protocol is up
  Internet address is 172.31.0.10/29, Area 0
  Process ID 1, Router ID 172.31.0.5, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.31.0.6
  Suppress hello for 0 neighbor(s)
```

FASE II: CONFIGURACIÓN AVANZADA DE OSPF:

1. El router Centro deberá ser DR y el router Norte, el BDR, evitando que un router nuevo ingrese y reemplace al DR.
2. Varíe los intervalos del Hello y dead.
3. Verifique las rutas internas y externas OSPF.
4. Verifique la conectividad desde diferentes Hosts.
5. Configuración activa.

DESARROLLO DE FASE II:

1. El router Centro, DR y router Norte, BDR.
   - Para la elección del DR es necesaria la prioridad del router o el ID del router, por lo que podemos modificar ambos datos o uno de ellos y de preferencia, la prioridad.
   - Un valor de prioridad 0 no permite al router participar, pero un valor desde 1 a 255, si. En este caso al router Norte se le define con el valor de 254 y al router Centro, con 255.

```
NORTE(config)#inter f1/0
NORTE(config-if)#ip ospf priority 254
NORTE(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
```

- Se verifica en la interfaz modificada el valor de prioridad.

```
NORTE#sh ip ospf interface f1/0
FastEthernet1/0 is up, line protocol is up
  Internet address is 172.31.0.5/29, Area 0
  Process ID 1, Router ID 172.31.0.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 254
  Designated Router (ID) 172.31.0.6, Interface address 172.31.0.6
  Backup Designated Router (ID) 172.31.0.5, Interface address 172.31.0.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
……..< resultado omitido>…….
```

- La tabla de vecinos aún no indicará cambio alguno, sólo se añade el valor de prioridad. En este caso el valor de 255 corresponde al router Centro.

```
NORTE#sh ip ospf nei
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.1.1      255   FULL/DROTHER    00:00:38    172.31.0.2      FastEthernet1/0
172.31.16.1       1   FULL/DR         00:00:38    172.31.0.1      FastEthernet1/0
172.31.12.1       1   FULL/-          00:00:39    172.31.0.18     Serial2/0
172.31.1.1        1   FULL/-          00:00:39    172.31.0.9      Serial3/0
```

- El proceso OSPF debe reiniciarse para permitir la nueva elección, incluso esto será necesario si el router tiene un nuevo ID o se le quiere modificar.

```
SUR#sh ip ospf nei
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.1.1      255   FULL/DROTHER    00:00:39    172.31.0.2      FastEthernet7/0
172.31.8.1      254   FULL/BDR        00:00:39    172.31.0.3      FastEthernet7/0
SUR#
```

2. Varíe los intervalos del Hello y defina los cálculos de costos más precisos.

- Se variaron los intervalos del hello en la interfaz 2/0 del router Norte, luego se verificó la interfaz.
- Debe realizarse en ambos puntos del enlace para mantener la adyacencia.

```
NORTE(config)#inter s2/0
NORTE(config-if)#ip ospf hello-interval 4
NORTE(config-if)#ip ospf dead-interval 15
NORTE(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
01:31:22: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.12.1 on Serial2/0 from EXCHANGE to FULL,
Exchange Done
NORTE#sh ip ospf inter s2/0
Serial2/0 is up, line protocol is up
  Internet address is 172.31.0.17/29, Area 0
  Process ID 1, Router ID 172.31.8.1, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 4, Dead 15, Wait 15, Retransmit 5
    Hello due in 00:00:03
……..< resultado omitido>…….
```

3. **TABLA DE ENRUTAMIENTO**:

- A diferencia del caso anterior existe la ruta de nivel 1 definida para alcanzar la red 198.98.9.0 /24 (router remoto) en el router Sur, así como la ruta por defecto definida en Lima para alcanzar Internet. Ambas rutas están redistribuidas hacia toda la topología OSPF.
- La rutas de nivel 2 son todas aquellas que están dentro del proceso OSPF.
- Las rutas etiquetadas como E2 son rutas externas de OSPF. En ellas, el (*) significa que son rutas por defecto.

```
LIMA#sh ip route
Gateway of last resort is 172.31.0.17 to network 0.0.0.0
C    20.0.0.0/8 is directly connected, Serial6/0
     172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
O       172.31.0.0/29 [110/782] via 172.31.0.17, 01:03:58, Serial3/0
O       172.31.0.8/29 [110/1562] via 172.31.0.17, 01:07:51, Serial3/0
C       172.31.0.16/29 is directly connected, Serial3/0
O       172.31.1.0/24 [110/783] via 172.31.0.17, 01:03:58, Serial3/0
O       172.31.4.0/23 [110/783] via 172.31.0.17, 01:03:58, Serial3/0
C       172.31.6.0/23 is directly connected, FastEthernet0/0
O       172.31.8.0/22 [110/782] via 172.31.0.17, 01:07:51, Serial3/0
C       172.31.12.0/22 is directly connected, FastEthernet1/0
O       172.31.16.0/22 [110/783] via 172.31.0.17, 01:03:58, Serial3/0
O E2 198.98.9.0/24 [110/20] via 172.31.0.17, 00:01:25, Serial3/0
S*   0.0.0.0/0 [1/0] via 172.31.0.17
```

```
ISP#sh ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial2/0
     172.31.0.0/18 is subnetted, 1 subnets
S       172.31.0.0 [1/0] via 10.1.1.1
C    198.98.9.0/24 is directly connected, Loopback0
```

```
NORTE#sh ip route
Gateway of last resort is 172.31.0.18 to network 0.0.0.0
     172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
C       172.31.0.0/29 is directly connected, FastEthernet1/0
C       172.31.0.8/29 is directly connected, Serial3/0
C       172.31.0.16/29 is directly connected, Serial2/0
O       172.31.1.0/24 [110/2] via 172.31.0.6, 01:06:57, FastEthernet1/0
O       172.31.4.0/23 [110/2] via 172.31.0.1, 01:06:57, FastEthernet1/0
O       172.31.6.0/23 [110/782] via 172.31.0.18, 01:10:46, Serial2/0
C       172.31.8.0/22 is directly connected, FastEthernet0/0
O       172.31.12.0/22 [110/782] via 172.31.0.18, 01:10:46, Serial2/0
O       172.31.16.0/22 [110/2] via 172.31.0.1, 01:06:57, FastEthernet1/0
O E2 198.98.9.0/24 [110/20] via 172.31.0.1, 00:04:20, FastEthernet1/0
O*E2 0.0.0.0/0 [110/1] via 172.31.0.18, 00:06:44, Serial2/0
```

```
SUR#SH IP ROUte
Gateway of last resort is 172.31.0.5 to network 0.0.0.0
C   10.0.0.0/8 is directly connected, Serial6/0
    172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
C      172.31.0.0/29 is directly connected, FastEthernet7/0
O      172.31.0.8/29 [110/782] via 172.31.0.5, 01:08:03, FastEthernet7/0
                     [110/782] via 172.31.0.6, 01:08:03, FastEthernet7/0
O      172.31.0.16/29 [110/782] via 172.31.0.5, 01:08:03, FastEthernet7/0
O      172.31.1.0/24 [110/2] via 172.31.0.6, 01:08:03, FastEthernet7/0
C      172.31.4.0/23 is directly connected, FastEthernet1/0
O      172.31.6.0/23 [110/783] via 172.31.0.5, 01:08:03, FastEthernet7/0
O      172.31.8.0/22 [110/2] via 172.31.0.5, 01:08:03, FastEthernet7/0
O      172.31.12.0/22 [110/783] via 172.31.0.5, 01:08:03, FastEthernet7/0
C      172.31.16.0/22 is directly connected, FastEthernet0/0
S   198.98.9.0/24 [1/0] via 10.1.1.2
O*E2 0.0.0.0/0 [110/1] via 172.31.0.5, 00:07:50, FastEthernet7/0
```

```
CENTRO#sh ip route
Gateway of last resort is 172.31.0.5 to network 0.0.0.0
    172.31.0.0/16 is variably subnetted, 9 subnets, 4 masks
C      172.31.0.0/29 is directly connected, FastEthernet1/0
C      172.31.0.8/29 is directly connected, Serial2/0
O      172.31.0.16/29 [110/782] via 172.31.0.5, 01:09:08, FastEthernet1/0
C      172.31.1.0/24 is directly connected, FastEthernet0/0
O      172.31.4.0/23 [110/2] via 172.31.0.1, 01:09:08, FastEthernet1/0
O      172.31.6.0/23 [110/783] via 172.31.0.5, 01:09:08, FastEthernet1/0
O      172.31.8.0/22 [110/2] via 172.31.0.5, 01:09:08, FastEthernet1/0
O      172.31.12.0/22 [110/783] via 172.31.0.5, 01:09:08, FastEthernet1/0
O      172.31.16.0/22 [110/2] via 172.31.0.1, 01:09:08, FastEthernet1/0
O E2 198.98.9.0/24 [110/20] via 172.31.0.1, 00:06:30, FastEthernet1/0
O*E2 0.0.0.0/0 [110/1] via 172.31.0.5, 00:08:54, FastEthernet1/0
```

4. DIAGNÓSTICO

- Prueba de conectividad desde un Host de la Lan de Lima hacia la topología.

```
PC>ping 172.31.1.10
Pinging 172.31.1.10 with 32 bytes of data:
Reply from 172.31.1.10: bytes=32 time=219ms TTL=125
Reply from 172.31.1.10: bytes=32 time=203ms TTL=125
Reply from 172.31.1.10: bytes=32 time=220ms TTL=125
Reply from 172.31.1.10: bytes=32 time=129ms TTL=125
Ping statistics for 172.31.1.10:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 129ms, Maximum = 220ms, Average = 192ms
PC>ping 198.98.9.8
Pinging 198.98.9.8  with 32 bytes of data:
Reply from 198.98.9.8 : bytes=32 time=220ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=233ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=156ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=187ms TTL=125
Ping statistics for 198.98.9.8 :
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 156ms, Maximum = 233ms, Average = 199ms
```

- Prueba de conectividad desde un Host de la Lan de Sur hacia la topología.

```
PC>ping 202.2.2.2
Pinging 202.2.2.2 with 32 bytes of data:
Reply from 202.2.2.2: bytes=32 time=209ms TTL=125
Reply from 202.2.2.2: bytes=32 time=203ms TTL=125
Reply from 202.2.2.2: bytes=32 time=200ms TTL=125
Reply from 202.2.2.2: bytes=32 time=209ms TTL=125
Ping statistics for 202.2.2.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 200ms, Maximum = 209ms, Average = 207ms
PC>ping 198.98.9.8
Pinging 198.98.9.8  with 32 bytes of data:
Reply from 198.98.9.8 : bytes=32 time=220ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=233ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=156ms TTL=125
Reply from 198.98.9.8 : bytes=32 time=187ms TTL=125
Ping statistics for 198.98.9.8 :
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 156ms, Maximum = 233ms, Average = 199ms
```

TAREAS

- Modificar los costos de los enlaces y verificar la métrica obtenida.

CONCLUSIONES Y/U OBSERVACIONES

Laboratorio N° 12 - Enrutamiento OSPF con rutas por defecto

INTRODUCCIÓN

La mayor parte de redes internas requiere de un enrutamiento de ruta por defecto hacia Internet, por lo que siempre será necesario diferenciar las diferentes aplicaciones que pudiera tener, adicionalmente si se tiene internamente un protocolo de enrutamiento como OSPF y, sumado a ello, el número de conexiones hacia Internet. Podría ser útil manejar el balanceo de carga en estas circunstancias, o las rutas de respaldo.

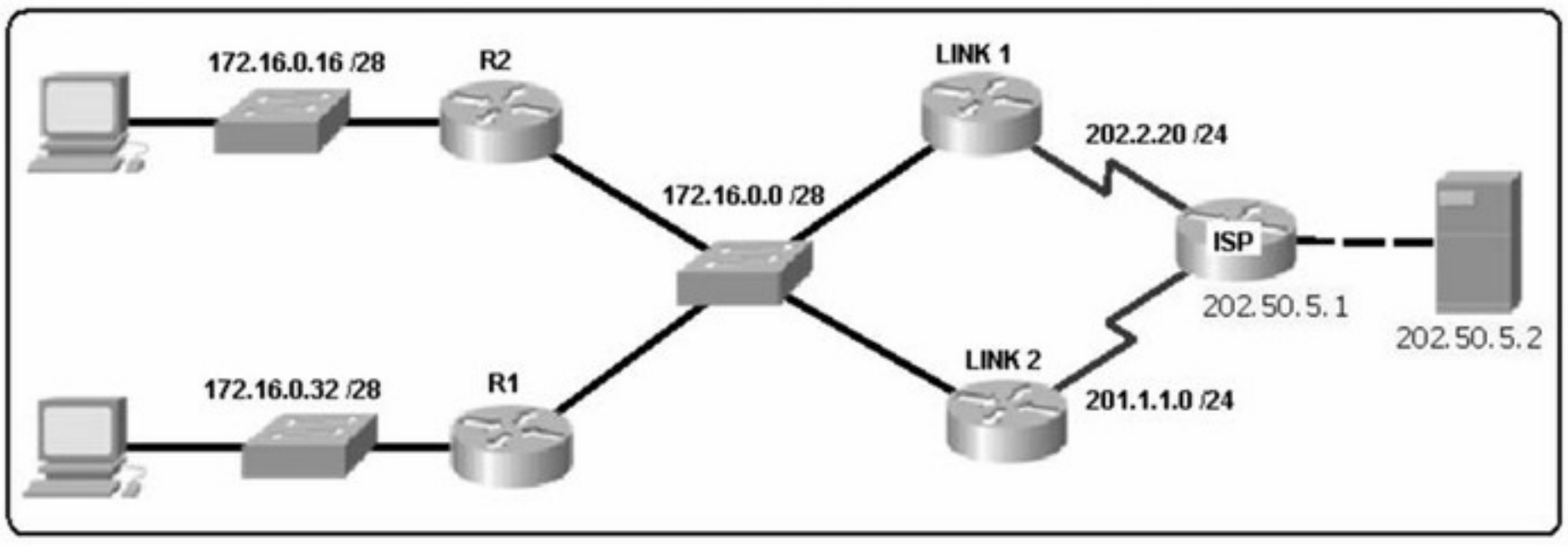
OBJETIVOS

- Configurar rutas por defecto y rutas estáticas con distinta distancia administrativa.
- Redistribuir las rutas por defecto mediante el protocolo OSPF.

DESCRIPCIÓN

El presente laboratorio tiene como propósito mantener dos enlaces hacia Internet, con la opción de tener un enlace principal y uno de respaldo.

En la configuración del laboratorio se utilizó la redistribución de la ruta por defecto de OSPF y rutas estáticas con distintas métricas para que no se realice el balance de carga y se mantenga liberado el enlace de respaldo.



DESARROLLO

1. **CONFIGURACIÓN FINAL**
   - El router LINK1 será el router de respaldo para la conexión a Internet, por lo que su ruta por defecto presenta un valor de distancia administrativa de 200 para no tomarse en cuenta inicialmente.
   - En su configuración también se definió la prioridad en 0 para no participar en la elección del DR.

```
LINK1#SH RUN
!
interface FastEthernet0/0
 ip address 172.16.20.3 255.255.255.248
 ip ospf priority 0
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 201.1.1.2 255.255.255.0
!
!
!
router ospf 1
 log-adjacency-changes
 network 172.16.20.0 0.0.0.15 area 0
 default-information originate
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 201.1.1.1 200
!
```

- A diferencia del router LINK1, la ruta por defecto del router LINK2 no presenta modificación de la distancia administrativa, de tal forma que al ser redistribuida mediante OSPF será considerada como ruta principal.
- En su configuración también se definió la prioridad en 0 para no participar en la elección del DR.

```
LINK2#SH RUN
!
!
interface FastEthernet0/0
 ip address 172.16.20.4 255.255.255.248
 ip ospf priority 0
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.0
!
!
router ospf 1
 log-adjacency-changes
 network 172.16.20.0 0.0.0.15 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 202.2.2.2
!
!
```

- El router R1 sólo requiere de la configuración del enrutamiento OSPF de sus dos subredes. Además, se habilitó la configuración DHCP para su red Lan.

- Para asegurar que este router sea definido como BDR se estableció una prioridad OSPF de 254 en la interfaz 0/0.

```
R1#SH RUN
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.248
 ip ospf priority 254
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.20.17 255.255.255.248
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 172.16.20.0 0.0.0.15 area 0
 network 172.16.20.16 0.0.0.15 area 0
!
ip classless
!
!
ip dhcp excluded-address 172.16.20.17 172.16.20.19
!
ip dhcp pool LAN1
 network 172.16.20.16 255.255.255.248
 default-router 172.16.20.17
!
```

- El router R2 requiere de la configuración del enrutamiento OSPF de sus dos subredes. Asimismo, se definió la prioridad en 255 para que el router sea elegido como DR.

```
R2#SH RUN
!
!
interface FastEthernet0/0
 ip address 172.16.20.2 255.255.255.248
 ip ospf priority 255
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.20.33 255.255.255.248
 ip helper-address 172.16.20.1
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 172.16.20.0 0.0.0.15 area 0
 network 172.16.20.32 0.0.0.15 area 0
!
!
```

- Para complementar la configuración y asignar al router LINK2 como ruta principal, se define su ruta sin variar la distancia administrativa, a diferencia de la ruta del router LINK1 donde se adiciona una distancia de 2.

```
ISP#sh run
!
!
interface FastEthernet0/0
 ip address 202.50.5.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 201.1.1.1 255.255.255.0
 clock rate 64000
!
interface Serial0/1
 ip address 202.2.2.2 255.255.255.0
 clock rate 64000
!
!
ip classless
ip route 172.16.20.0 255.255.255.0 Serial0/1
ip route 172.16.20.0 255.255.255.0 Serial0/0 2
!
!
```

2. **TABLA DE ENRUTAMIENTO**:
   - Adicionalmente a la correcta publicación de redes, obsérvese que en todos los routers el Gateway de último recurso es el router LINK2 con la dirección 172.16.20.4, incluido el router de respaldo.
   - Al recibirse la redistribución de la ruta por defecto también se indica la vía por donde alcanzamos Internet.

```
LINK1# SH IP ROUTE
Gateway of last resort is 172.16.20.4 to network 0.0.0.0
    172.16.0.0/29 is subnetted, 3 subnets
C       172.16.20.0 is directly connected, FastEthernet0/0
O       172.16.20.16 [110/2] via 172.16.20.1, 00:07:48, FastEthernet0/0
O       172.16.20.32 [110/2] via 172.16.20.2, 00:07:58, FastEthernet0/0
C    201.1.1.0/24 is directly connected, Serial0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.4, 00:06:34, FastEthernet0/0
```

```
R1# SH IP ROUTE
Gateway of last resort is 172.16.20.4 to network 0.0.0.0
    172.16.0.0/29 is subnetted, 3 subnets
C       172.16.20.0 is directly connected, FastEthernet0/0
C       172.16.20.16 is directly connected, FastEthernet0/1
O       172.16.20.32 [110/2] via 172.16.20.2, 00:24:34, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.4, 00:23:20, FastEthernet0/0
```

```
R2# SH IP ROUTE
Gateway of last resort is 172.16.20.4 to network 0.0.0.0
    172.16.0.0/29 is subnetted, 3 subnets
C       172.16.20.0 is directly connected, FastEthernet0/0
O       172.16.20.16 [110/2] via 172.16.20.1, 00:10:09, FastEthernet0/0
C       172.16.20.32 is directly connected, FastEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 172.16.20.4, 00:08:55, FastEthernet0/0
```

- En el caso del router LINK2 que se emplea como ruta principal, su Gateway de último recurso es su siguiente salto 202.2.2.2, que corresponde al router ISP.

```
LINK2#SH IP ROUTE
Gateway of last resort is 202.2.2.2 to network 0.0.0.0
    172.16.0.0/29 is subnetted, 3 subnets
C       172.16.20.0 is directly connected, FastEthernet0/0
O       172.16.20.16 [110/2] via 172.16.20.1, 00:08:12, FastEthernet0/0
O       172.16.20.32 [110/2] via 172.16.20.2, 00:08:12, FastEthernet0/0
C    202.2.2.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 202.2.2.2
```

3. **DIAGNÓSTICO**

- Desde el router R2 comprobamos la conectividad, además del trazado de ruta hacia el Host de Internet.

```
R2#PING 202.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 49/66/94 ms
```

```
R2#PING 202.50.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.50.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 78/93/109 ms
```

```
R2#TRACER 202.50.5.10
Type escape sequence to abort.
Tracing the route to 202.50.5.10
 1  172.16.20.4    62 msec  63 msec  62 msec
 2  202.2.2.2      94 msec  94 msec  94 msec
 3  202.50.5.10    125 msec 125 msec 93 msec
```

- Desde el router R1 comprobamos la conectividad, además del trazado de ruta hacia el Host de Internet.

```
R1#traceroute 201.1.1.1
Type escape sequence to abort.
Tracing the route to 201.1.1.1
 1  172.16.20.4    21 msec  7 msec   8 msec
 2  202.2.2.2      10 msec  10 msec  15 msec
```

```
R1#traceroute 201.1.1.2
Type escape sequence to abort.
Tracing the route to 201.1.1.2
 1  172.16.20.4    23 msec  7 msec   10 msec
 2  202.2.2.2      12 msec  16 msec  12 msec
 3  201.1.1.2      13 msec  13 msec  10 msec
```

CONCLUSIONES Y/U OBSERVACIONES

_____

REDES WAN

Corresponde a la configuración de soluciones que presentan los proveedores de servicio, profundizando en el trabajo de la tecnología Frame Relay junto con los protocolos de enrutamiento OSPF y EIGRP, el encapsulamiento PPP con autenticación, y los servicios de traducción de direcciones (NAT).

LABORATORIO N° 1: PPP y RIP v2

La implementación del laboratorio tiene por finalidad la de habilitar el enrutamiento RIP dentro de dos topologías de conexión hacia Internet, las cuales se comunican mediante rutas por defecto. El enlace de conexiones WAN se realiza con el encapsulamiento PPP y su autenticación.

LABORATORIO N° 2: DHCP Y NAT

Se establece la configuración en un router como servidor DHCP, además de habilitar secuencialmente el servicio de traducción de direcciones de modo dinámico (NAT).

LABORATORIO N° 3: NAT ESTÁTICO Y DE SOBRECARGA

El laboratorio proyecta utilizar un doble servicio de traducción estableciendo un esquema con la operación de NAT dinámico y NAT de sobrecarga sobre un proceso de enrutamiento OSPF y su conexión a Internet.

LABORATORIO N° 4: TOPOLOGIA HUB AND SPOKE CON SPLIT HORIZON

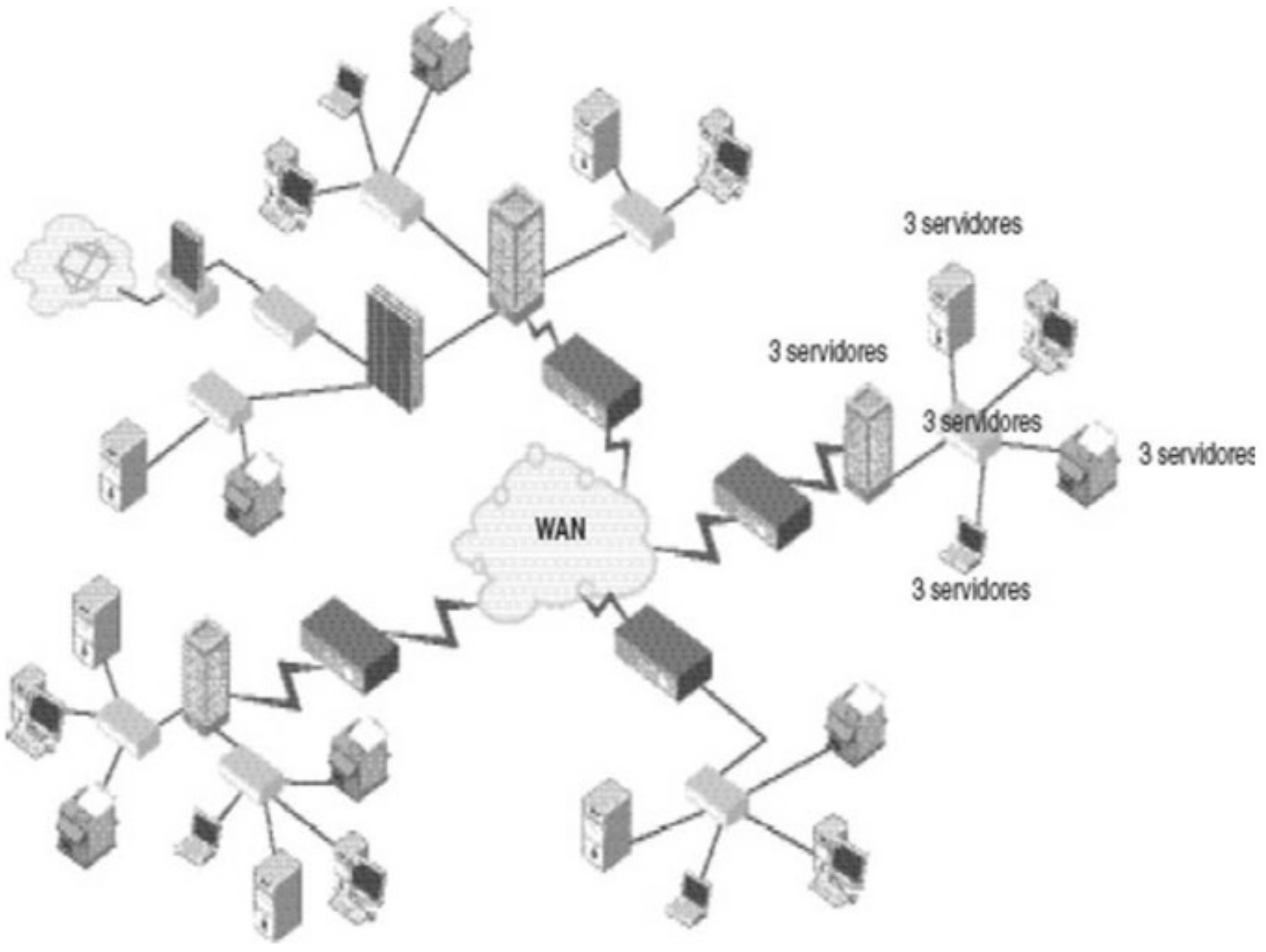
La tecnología Frame Relay es representada mediante dispositivos Cisco para formar la topología Hub and Spoke donde, en un primer caso, se habilita un router como switch Frame Relay y se encapsulan las interfaces seriales de los routers con enrutamiento EIGRP. En un segundo caso, se modifica la configuración para el uso de subinterfaces.

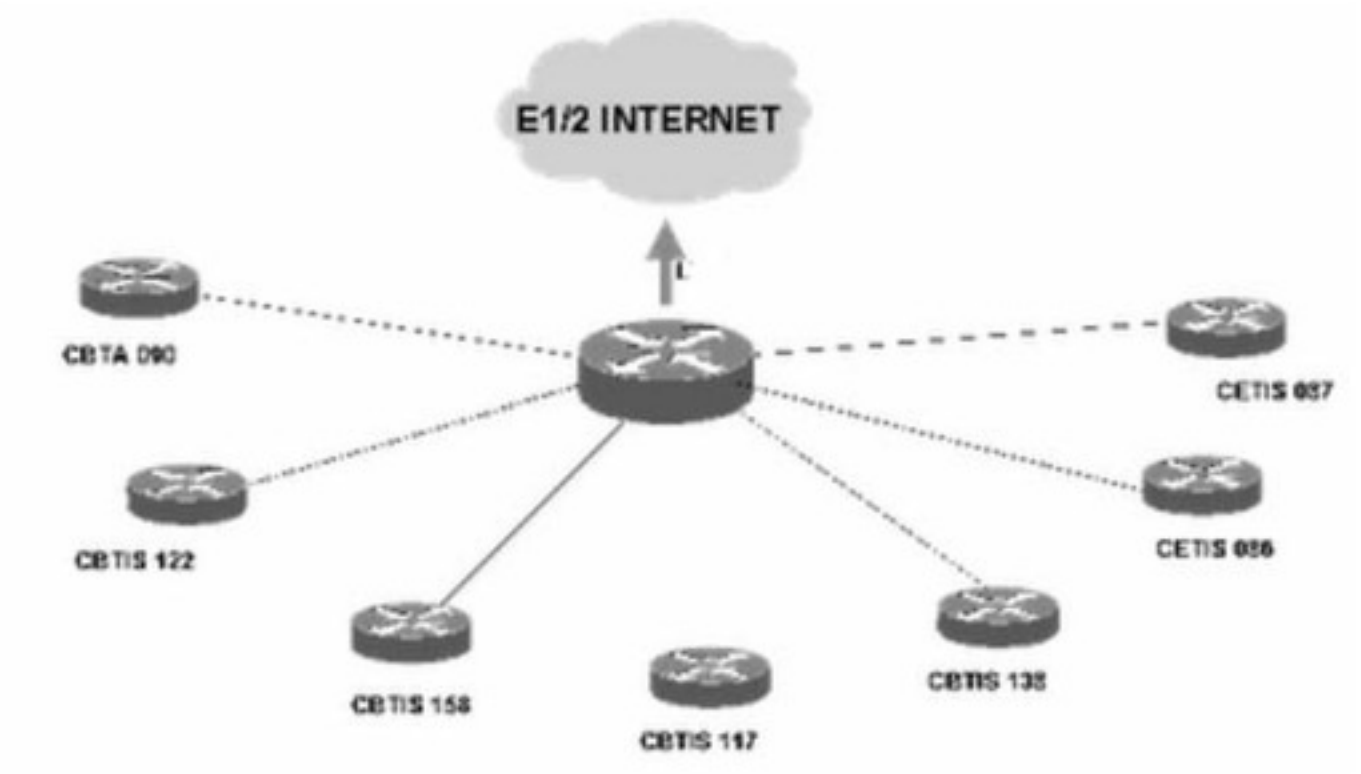
LABORATORIO N° 5: TOPOLOGÍA NBMA

El laboratorio se establece en una red NBMA, con la configuración de un switch Frame Relay y dividido en tres casos. El primero es la implementación del enrutamiento EIGRP con la sumarización de rutas y la redistribución de la ruta por defecto. El segundo caso trabaja con OSPF, donde se debe agregar el vecino ospf y establecer el DR y BDR. El tercer caso opera con el protocolo RIP v2 y se verifica su funcionamiento.

LABORATORIO N° 6: TOPOLOGÍAS MULTIPUNTO Y PUNTO – MULTIPUNTO

Se desarrolla la tecnología Frame Relay en dos casos: con una red multipunto y una red punto – multipunto con una implementación del protocolo de OSPF.


3 servidores
3 servidores
3 servidores
3 servidores
3 servidores
WAN


E1/2 INTERNET
CBTA 090
CETIS 037
CBTIS 122
CETIS 056
CBTIS 158
CBTIS 117
CBTIS 138

Capítulo

3 Redes Wan

LABORATORIO N° 1 - PPP y RIP v2

INTRODUCCIÓN

Protocolo punto a punto (PPP) es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Es un protocolo asociado a la pila TCP/IP de uso en Internet.

El protocolo PPP permite establecer una comunicación a nivel de enlace. Se utiliza normalmente para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita la autenticación y la asignación dinámica de direcciones.

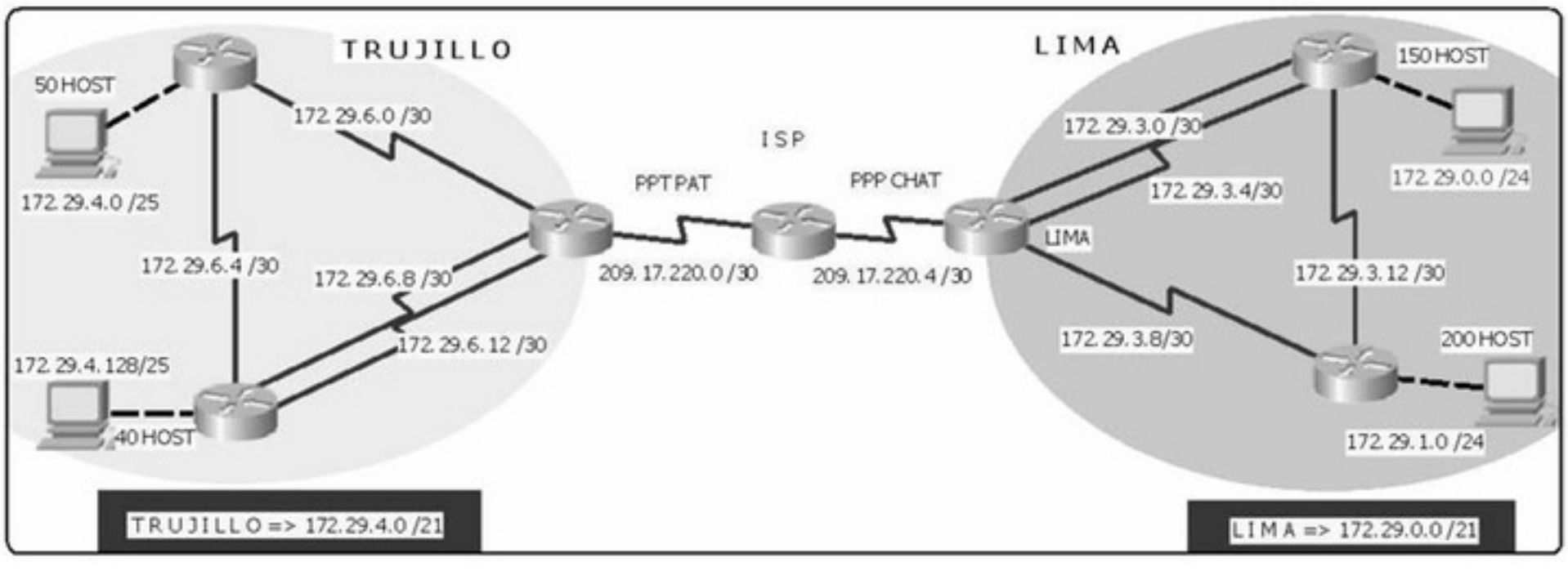
OBJETIVOS

- Complementar el funcionamiento del protocolo de enrutamiento RIP con el encapsulamiento PPP.

DESCRIPCIÓN

La implementación del siguiente laboratorio tiene por finalidad habilitar el enrutamiento RIP en cada ciudad y comunicarlos mediante rutas por defecto hacia Internet.

El ISP presenta dos conexiones WAN mediante encapsulamiento PPP con autenticación hacia los routers LIMA_1 y TRUJILLO_1.



DESARROLLO

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

FASE 1: CONFIGURACIÓN BÁSICA

a. Realice las conexiones y elimine la configuración de cada router, en caso la tenga.
b. Habilite la opción de captura de texto en el Hyperterminal.
c. Realice la configuración básica con ayuda del editor de texto.

FASE 2: HABILITAR ENRUTAMIENTO

a. Los routers de la topología, excepto el router ISP, no habilitan el protocolo RIP. Los routers de la ciudad de Trujillo habilitan una configuración de enrutamiento similar a la de la ciudad de Lima.
b. El router ISP deberá tener una ruta estática hacia cada red interna para facilitar su acceso, como se muestra en la tabla de enrutamiento.

```
ISP#sh ip route
Gateway of last resort is not set
     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0 [1/0] via 209.17.220.5
S       172.29.4.0 [1/0] via 209.17.220.1
     209.17.220.0/30 is subnetted, 2 subnets
C       209.17.220.0 is directly connected, Serial0/0/0
C       209.17.220.4 is directly connected, Serial0/0/1
```

c. Los routers Lima_1 y Trujillo_1 deberán habilitar una ruta por defecto dirigida hacia Internet y redistribuirla mediante el enrutamiento RIP.
d. Obsérvese en su tabla de enrutamiento que se tiene agregada dicha ruta en cada router.
e. Asimismo, se muestran las redes recibidas, como también la doble y triple vía a las redes de acuerdo a su ubicación.

```
TRUJILLO_1#SH IP ROUTE
Gateway of last resort is 209.17.220.2 to network 0.0.0.0
     172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:17, Serial0/0/0
R       172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:15, Serial0/1/1
                        [120/1] via 172.29.6.10, 00:00:15, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
R       172.29.6.4/30 [120/1] via 172.29.6.2, 00:00:17, Serial0/0/0
                      [120/1] via 172.29.6.14, 00:00:15, Serial0/1/1
                      [120/1] via 172.29.6.10, 00:00:15, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/0/1
C       172.29.6.12/30 is directly connected, Serial0/1/1
     209.17.220.0/30 is subnetted, 1 subnets
C       209.17.220.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.17.220.2
```

```
LIMA_1#sh ip route
Gateway of last resort is 209.17.220.6 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R      172.29.0.0/24 [120/1] via 172.29.3.6, 00:00:01, Serial0/1/1
                     [120/1] via 172.29.3.2, 00:00:01, Serial0/0/1
R      172.29.1.0/24 [120/1] via 172.29.3.10, 00:00:06, Serial0/1/0
C      172.29.3.0/30 is directly connected, Serial0/0/1
C      172.29.3.4/30 is directly connected, Serial0/1/1
C      172.29.3.8/30 is directly connected, Serial0/1/0
R      172.29.3.12/30 [120/1] via 172.29.3.6, 00:00:01, Serial0/1/1
                      [120/1] via 172.29.3.2, 00:00:01, Serial0/0/1
                      [120/1] via 172.29.3.10, 00:00:06, Serial0/1/0
    209.17.220.0/30 is subnetted, 1 subnets
C      209.17.220.4 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.6
```

f. En el caso de los routers siguientes, la recepción de publicaciones RIP no debe tener inconvenientes, sólo deberá comprobarse que se muestren todas las rutas hacia las redes de acuerdo a su ubicación.

```
TRUJILLO_2#sh ip route
Gateway of last resort is 172.29.6.1 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.29.4.0/25 is directly connected, FastEthernet0/0
R      172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
C      172.29.6.0/30 is directly connected, Serial0/0/0
C      172.29.6.4/30 is directly connected, Serial0/0/1
R      172.29.6.8/30 [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
                     [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
R      172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
                      [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
```

```
TRUJILLO_3#sh ip route
Gateway of last resort is 172.29.6.13 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R      172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:17, Serial0/0/1
C      172.29.4.128/25 is directly connected, FastEthernet0/0
R      172.29.6.0/30 [120/1] via 172.29.6.13, 00:00:16, Serial0/1/0
                     [120/1] via 172.29.6.5, 00:00:17, Serial0/0/1
                     [120/1] via 172.29.6.9, 00:00:16, Serial0/0/0
C      172.29.6.4/30 is directly connected, Serial0/0/1
C      172.29.6.8/30 is directly connected, Serial0/0/0
C      172.29.6.12/30 is directly connected, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:16, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:16, Serial0/0/0
```

```
LIMA_3#sh ip route
Gateway of last resort is 172.29.3.5 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.29.0.0/24 is directly connected, FastEthernet0/0
R       172.29.1.0/24 [120/1] via 172.29.3.14, 00:00:01, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/1/0
R       172.29.3.8/30 [120/1] via 172.29.3.5, 00:00:27, Serial0/1/0
                      [120/1] via 172.29.3.1, 00:00:27, Serial0/0/0
                      [120/1] via 172.29.3.14, 00:00:01, Serial0/0/1
C       172.29.3.12/30 is directly connected, Serial0/0/1
R*  0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:27, Serial0/1/0
R*  0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:27, Serial0/0/0
```

```
LIMA_2#sh ip rout
Gateway of last resort is 172.29.3.9 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.29.0.0/24 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
C       172.29.1.0/24 is directly connected, FastEthernet0/0
R       172.29.3.0/30 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
                      [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
R       172.29.3.4/30 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
                      [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
C       172.29.3.8/30 is directly connected, Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/0/1
R*  0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
```

FASE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO RIP

- El comando **passive-interface** es empleado para evitar la publicación de actualizaciones.
- Para realizar esta configuración puede usar el comando **passive-interface default**, el cual desactiva la publicación por todas las interfaces, y luego debería habilitarse cada interfaz. A continuación, una lista de las interfaces en las que debería permitirse la publicación.

ROUTER	INTEFAZ
LIMA_1	SERIAL 0/0/1, 0/1/0, 0/1/1
LIMA_2	SERIAL 0/0/0, 0/0/1
LIMA_3	SERIAL 0/0/0, 0/0/1, 0/1/0
TRUJILLO_1	SERIAL 0/0/0, 0/0/1, 0/1/1
TRUJILLO_2	SERIAL 0/0/0, 0/0/1
TRUJILLO_3	SERIAL 0/0/0, 0/0/1, 0/1/0
ISP	No lo requiere

FASE 4: CONFIGURAR ENCAPSULAMIENTO PPP

- Para este caso sólo deberán configurarse los routers Lima_1, Trujillo_1 y el ISP.
- Se muestra a continuación la configuración final de cada router.
- Obsérvese que entre los routers ISP y Lima_1 deberá tenerse encapsulamiento PPP con autenticación PAT. Mientras que entre los routers ISP y Trujillo_1, el encapsulamiento PPP tendrá autenticación CHAT.

```
ISP#sh runn
!
!
username LIMA_1 password 0 seguridad456
username TRUJILLO_1 password 0 seguridad123
!
!
interface Serial0/0/0
 ip address 209.17.220.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username ISP password 0 seguridad123
!
interface Serial0/0/1
 ip address 209.17.220.6 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
!
ip classless
ip route 172.29.0.0 255.255.252.0 209.17.220.1
ip route 172.29.4.0 255.255.252.0 209.17.220.5
!
!
```

```
TRUJILLO_1#sh run
!
!
username ISP password 0 seguridad123
!
!
interface Serial0/0/0
 ip address 172.29.6.1 255.255.255.252
!
interface Serial0/0/1
 ip address 172.29.6.9 255.255.255.252
!
interface Serial0/1/0
 ip address 209.17.220.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username TRUJILLO_1 password 0 seguridad123
 clock rate 64000
!
interface Serial0/1/1
 ip address 172.29.6.13 255.255.255.252
 clock rate 64000
!
router rip
 version 2
 passive-interface Serial0/1/0
 network 172.29.0.0
 default-information originate
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.2
!
!
```

```
LIMA_1#sh runn
!
!
username ISP password 0 seguridad456
!
!
interface Serial0/0/0
 ip address 209.17.220.5 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 ip address 172.29.3.1 255.255.255.252
 clock rate 64000
!
interface Serial0/1/0
 ip address 172.29.3.9 255.255.255.252
 clock rate 64000
!
interface Serial0/1/1
 ip address 172.29.3.5 255.255.255.252
!
!
router rip
 version 2
 passive-interface Serial0/0/0
 network 172.29.0.0
 default-information originate
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.6
!
!
```

- Se muestra la configuración final que deberían tener los demás routers.

```
TRUJILLO_2#sh runn
!
interface FastEthernet0/0
 ip address 172.29.4.1 255.255.255.128
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.29.6.2 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
```

```
 ip address 172.29.6.5 255.255.255.252
 clock rate 64000
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
!
```

```
TRUJILLO_3#sh run
!
!
interface FastEthernet0/0
 ip address 172.29.4.129 255.255.255.128
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.29.6.10 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.29.6.6 255.255.255.252
!
interface Serial0/1/0
 ip address 172.29.6.14 255.255.255.252
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
```

```
LIMA_3#sh runn
!
!
interface FastEthernet0/0
 ip address 172.29.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.29.3.2 255.255.255.252
!
interface Serial0/0/1
 ip address 172.29.3.13 255.255.255.252
 clock rate 64000
!
interface Serial0/1/0
 ip address 172.29.3.6 255.255.255.252
 clock rate 64000
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
!
```

```
LIMA_2#sh run
!
!
interface FastEthernet0/0
 ip address 172.29.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.29.3.10 255.255.255.252
!
interface Serial0/0/1
 ip address 172.29.3.14 255.255.255.252
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
!
```

TAREAS:

- Habilitar la autenticación en el enrutamiento RIP de Trujillo.
- Habilitar el enrutamiento OSPF en los routers de Lima.
- Habilitar NAT con sobrecarga en el router Lima_1.

CONCLUSIONES

_____

_____

_____

_____

Laboratorio N° 2 - DHCP y NAT

INTRODUCCIÓN

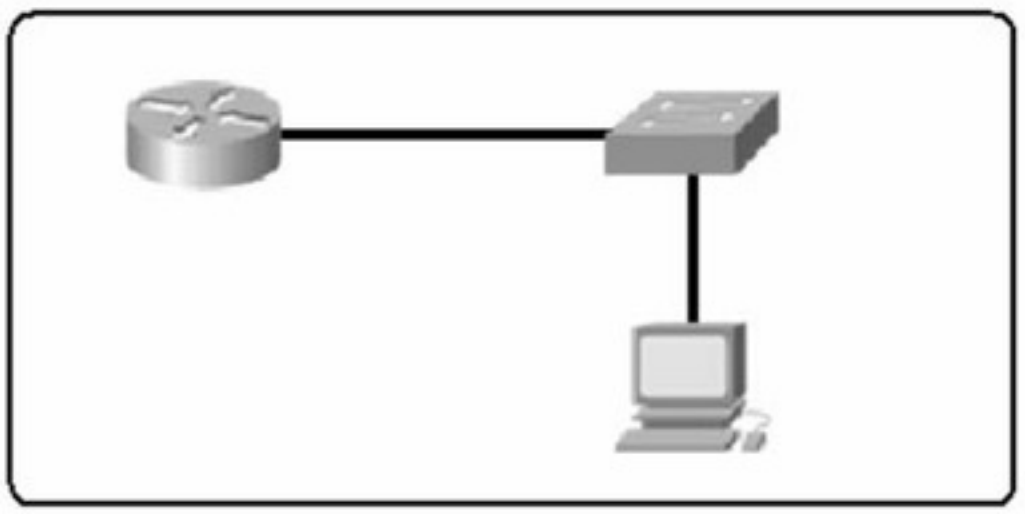
Toda máquina perteneciente a una red cuya pila de protocolos sea TCP/IP necesita que se le asigne una dirección IP, ya sea de manera estática o dinámica, antes de que ésta pueda intercambiar datagramas IP. En la arquitectura TCP/IP se cuenta con el protocolo *Dynamic Host Configuration Protocol* (DHCP). Este protocolo, que funciona bajo el paradigma cliente – servidor, permite que los clientes de una red obtengan sus configuraciones de red a partir de un servidor DHCP.

NAT (*Network Address Translation*): Está diseñado para conservar las direcciones IP públicas y permitir que las redes utilicen direcciones IP privadas en las redes internas.

OBJETIVOS

- Configurar un router como servidor DHCP.
- Configurar NAT en routers y observar su funcionalidad.

PROCEDIMIENTO



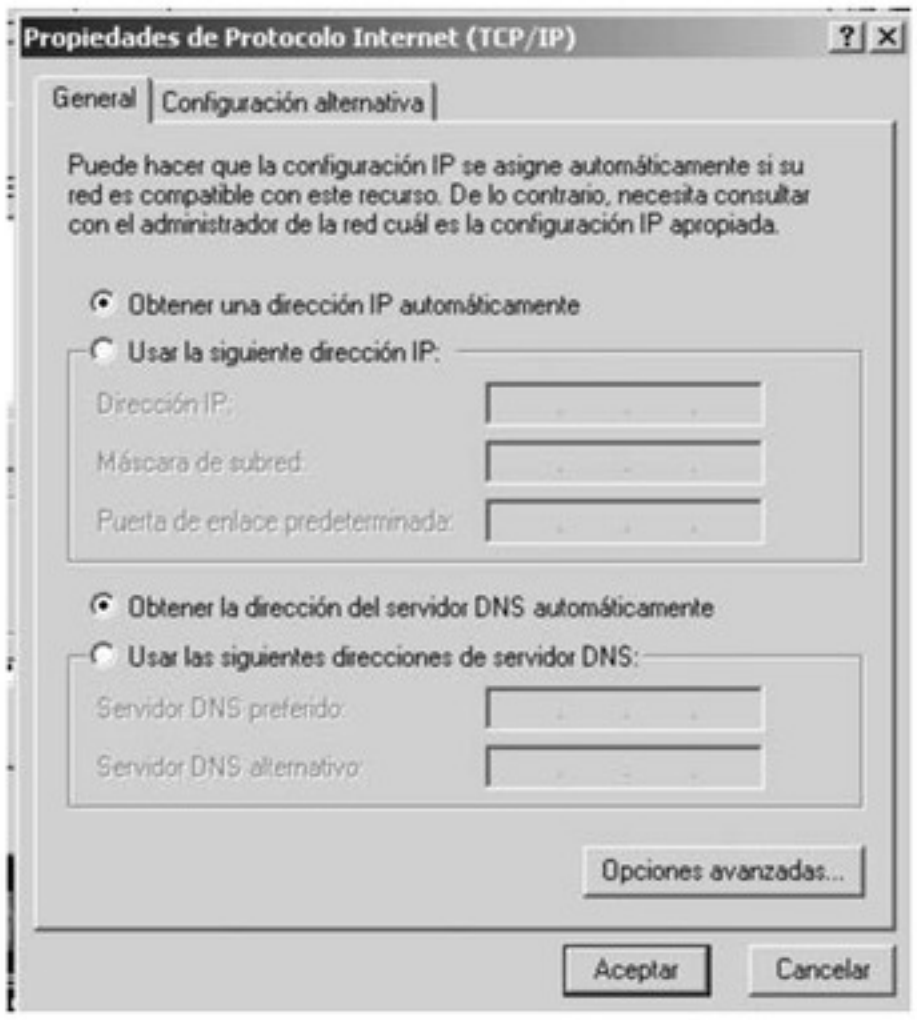
1. Realice las rutinas de diagnóstico y deje listos los equipos para su configuración.
2. Realice la conexión física de los equipos en base a la topología de red.
3. Habilite la opción de captura de texto en el emulador (Hyperterminal).
4. Realice la configuración básica del equipo con ayuda del bloc de notas.
5. Configure DHCP en el router.

```
Router# configure terminal
Router(config)# ip dhcp pool campus
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.2
```

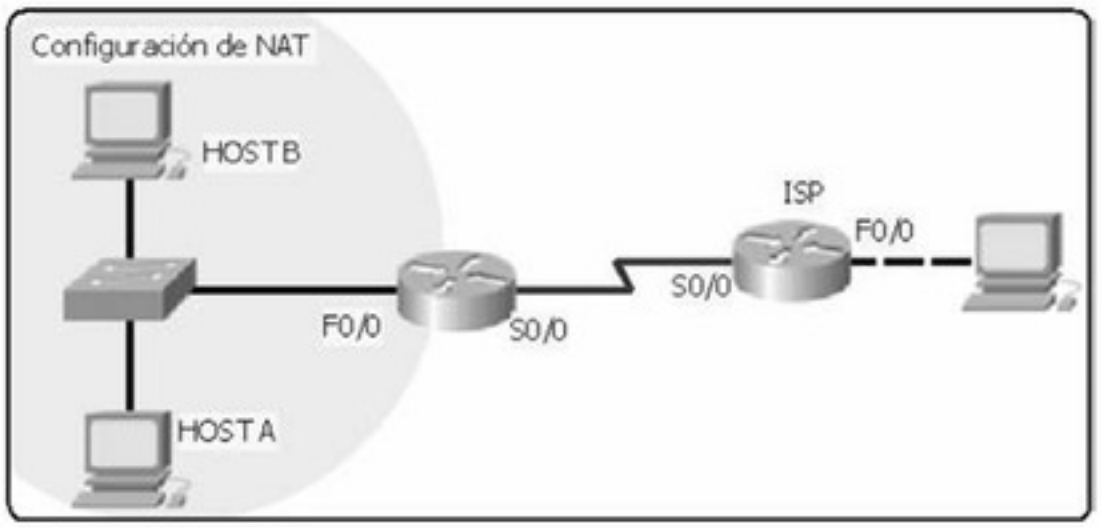
6. Para excluir un conjunto de direcciones del pool creado use:

```
Router(config)# ip dhcp excluded 192.168.1.1 192.168.1.10
```

7. Verifique el funcionamiento de DHCP. Para eso configure su PC para que obtenga una dirección IP de forma dinámica. La gráfica ilustra el proceso:


Propiedades de Protocolo Internet (TCP/IP)
General
Configuración alternativa
Puede hacer que la configuración IP se asigne automáticamente si su red es compatible con este recurso. De lo contrario, necesita consultar con el administrador de la red cuál es la configuración IP apropiada.
Obtener una dirección IP automáticamente
Usar la siguiente dirección IP:
Dirección IP:
Máscara de subred:
Puerta de enlace predeterminada:
Obtener la dirección del servidor DNS automáticamente
Usar las siguientes direcciones de servidor DNS:
Servidor DNS preferido:
Servidor DNS alternativo:
Opciones avanzadas...
Aceptar
Cancelar

Configuración de NAT



8. Inicie una sesión con Hyperterminal y configure los siguientes aspectos en el router etiquetado en la figura 1 como NAT. Haga lo mismo con ISP.
   a. Nombre del router.
   b. Configure una contraseña para pasar de modo usuario a modo privilegiado.
   c. Configure el router para ser accedido vía Telnet.

9. Configure la interfaz Serial 0/0 de NAT e ISP de la siguiente manera:

```
NAT# configure terminal
NAT(config)#interface serial 0/0
NAT(config- if)#ip address 200.12.180.1 255.255.255.0
NAT(config- if)#clock rate 64000
NAT(config-if)#no shutdown
```

```
ISP#configure terminal
ISP(config)#interface serial 0/0
ISP(config- if)#ip address 200.12.180.2 255.255.255.0
ISP(config- if)#no shutdown
```

10. Configure las direcciones FastEthernet de NAT e ISP de la siguiente manera:

```
NAT# configure terminal
NAT(config)#interface fastethernet 0/0
NAT(config- if)#ip address 192.168.1.1 255.255.255.0
NAT(config-if)#no shutdown
```

```
ISP#configure terminal
ISP(config)#interface fastethernet 0/0
ISP(config- if)#ip address 200.200.50.1 255.255.255.0
ISP(config-if)#no shutdown
```

11. Configure una ruta estática hacia Internet en el router NAT:

```
NAT#config terminal
NAT(config)#ip route 0.0.0.0 0.0.0.0 200.12.180.2
```

12. Cree la siguiente ruta estática en el router ISP:

```
ISP#config terminal
ISP(config)#ip route 200.200.100.128 255.255.255.128 200.12.180.1
```

13. Cree la siguiente lista de control de acceso para definir a los usuarios:

```
NAT# configure terminal
NAT(config)#access- list 1 permit 192.168.1.0 255.255.255.0
```

14. A continuación procederemos a configurar NAT de manera estática, de tal forma que se mapeará la dirección 192.168.1.2 a la dirección 200.200.100.252. Digite el siguiente comando sobre el router NAT:

```
NAT#configure terminal
NAT(config)#ip nat inside source static 192.168.1.2 200.200.100.252
```

15. A continuación procederemos a configurar NAT de manera dinámica. Para esto tendremos que configurar un pool de direcciones e indicar al router que haga el mapeo de una dirección del pool a una dirección privada perteneciente a un Host. Para efectos de este laboratorio se realizará un mapeo no estático de los Hosts pertenecientes al segmento de red 192.168.1.0 /24 a las direcciones de red 200.200.100.129 a 200.12.100.250.

```
NAT#configure terminal
NAT(config)#ip nat pool dir_Publicas 200.200.100.129 200.200.100.250 netmask 255.255.255.128
NAT(config)# ip nat inside source list 1 pool dir_Publicas
```

16. El último comando digitado provee de una traducción de uno a uno entre una dirección pública del pool creado (dir_Públicas) y una dirección IP privada especificada por la lista de control de acceso (access- list 1).

17. Ahora procedemos a configurar la interfaz INSIDE y OUTSIDE; en este caso, la interfaz FastEthernet 0/0 es la interfaz INSIDE mientras que la interfaz Serial 0/0 es la interfaz OUTSIDE.

```
NAT#configure terminal
NAT(config)#interface fastethernet 0/0
NAT(config- if)#ip nat inside
NAT(config- if)#interface serial 0/0
NAT(config- if)#ip nat outside
```

18. Configuración final de cada router.

```
ISP#SH RUN
!
!
interface FastEthernet0/0
 ip address 200.200.50.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.12.180.2 255.255.255.0
!
!
ip classless
ip route 200.200.100.128 255.255.255.128 200.12.180.1
!
!
```

```
NAT#SH RUN
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.12.180.1 255.255.255.0
 ip nat outside
 clock rate 64000
!
!
```

```
ip nat pool dir_Publicas 200.200.100.129 200.200.100.250 netmask 255.255.255.128
ip nat inside source list 1 pool dir_Publicas
ip nat inside source static 192.168.1.2 200.200.100.252
ip classless
ip route 0.0.0.0 0.0.0.0 200.12.180.2
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool campus
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.2
!
```

CONCLUSIONES Y/U OBSERVACIONES

LABORATORIO N° 3 - NAT ESTÁTICO Y DE SOBRECARGA

INTRODUCCIÓN

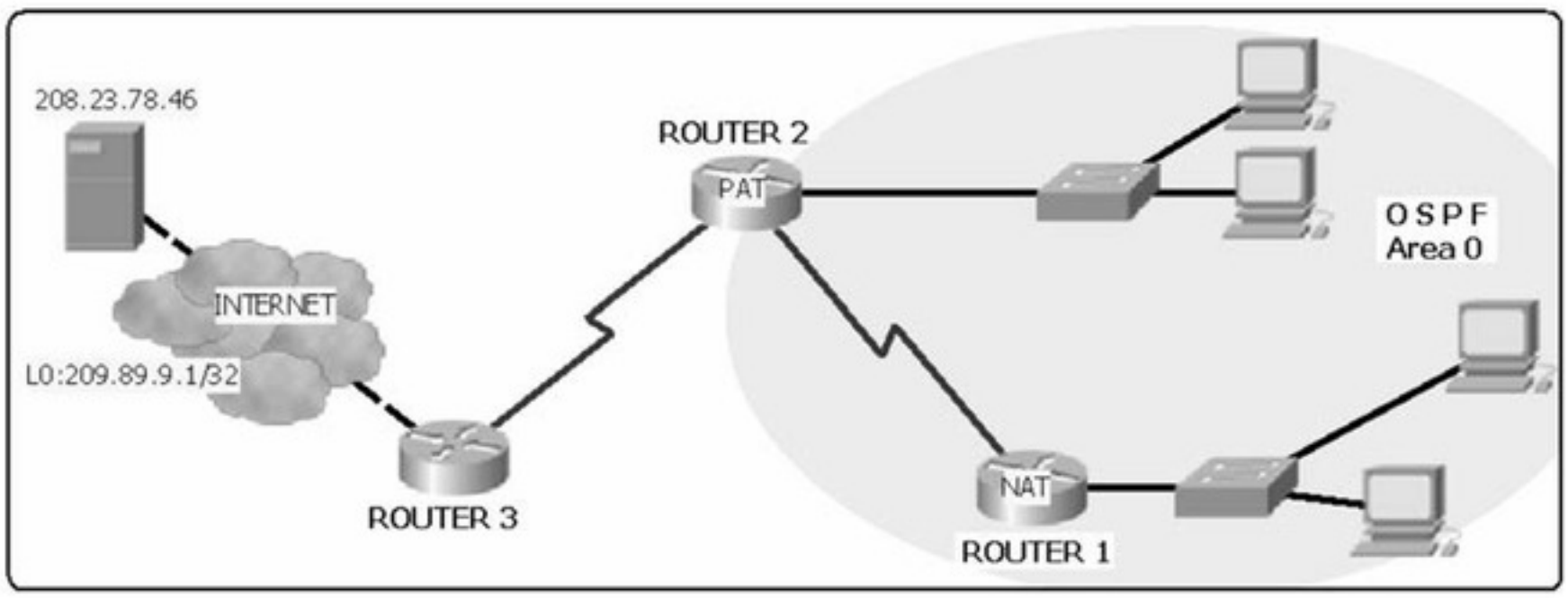
El servicio NAT es un mecanismo utilizado por dispositivos de enrutamiento IP entre dos redes que se asignan mutuamente direcciones para intercambiar paquetes. Consiste en pasar de un extremo a otro las direcciones utilizadas de los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

OBJETIVOS

- Establecer un esquema que facilite la operación de NAT dinámico con el NAT de sobrecarga sobre un proceso de enrutamiento OSPF y su conexión a Internet.

DESCRIPCIÓN

El laboratorio pretende utilizar un doble servicio NAT que permita ocultar redes o facilitar la implementación de nuevas redes donde los problemas de crecimiento son una dificultad considerable.



- En caso de acelerar el proceso de configuración, se adjunta un archivo que se podría copiar desde el disco que acompaña al presente texto, en él encontrará la configuración hasta antes de habilitar el enrutamiento.
- Para realizar una configuración más adecuada verifique las interfaces seriales y Ethernet.

1. Realice las rutinas de diagnóstico y deje listos los equipos para su configuración.
2. Realice la conexión física de los equipos en base a la topología de red.
3. Habilite la opción de captura de texto en el emulador (Hyperterminal).
4. Realice el cálculo por VLSM de la siguiente configuración.

Router	Nombre	Nº de host	Otros
1	SUR	20	Crecimiento del 50%
2	CENTRO	20	Crecimiento del 50%
3	ISP	-----	----

5. Realice la configuración básica y configuración avanzada mediante el enrutamiento OSPF.
6. En el caso de NAT se debe realizar una doble traducción, como sigue:
   a. El router 1 debe traducir las direcciones de su red privada mediante NAT.
   b. El router 2 debe traducir las direcciones de su red privada mediante PAT.
   c. Ambos deben tener salida hacia Internet.

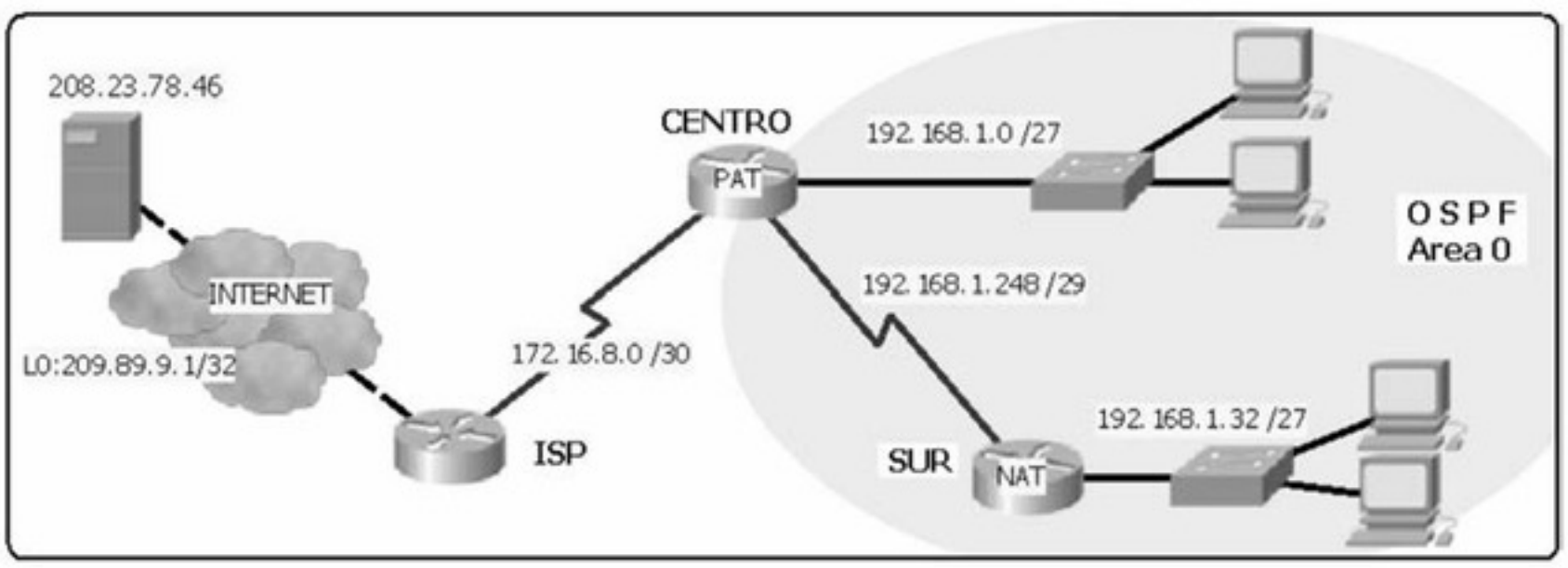
DESARROLLO

El direccionamiento IP que se plantea da solución a los requisitos exigidos, donde la dirección 192.168.1.0 /24 es utilizada para el proceso OSPF.

El planteamiento requiere de una solución por partes, considerando primero el enrutamiento OSPF donde sólo se deben publicar las redes que operarán sin NAT dentro del área 0, es decir, la red Lan del router 2 y el enlace entre el router 1 y el router 2.

Posteriormente habilitaremos el servicio NAT en el router Sur para que su red Lan acceda a la red OSPF con direcciones de la subred que ya esté ruteada, en este caso: 192.168.1.248/29 (192.168.1.249 a 192.168.1.252).

Finalmente habilitamos PAT en el router Centro para facilitar que toda la red 192.168.1.0 /24 pueda acceder a Internet empleando la dirección de la interfaz serial 0/0.



FASE 1: CONFIGURACIÓN DEL ENRUTAMIENTO:

- El router Sur necesita configurar OSPF para la publicación de la subred de la interfaz serial 0/0.

```
SUR#SH RUN
!
!
interface Loopback0
 ip address 209.9.9.9 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.33 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
```

```
 speed auto
 shutdown
!
interface Serial0/0
 ip address 192.168.1.253 255.255.255.248
 !
!
router ospf 1
 log-adjacency-changes
  network 192.168.1.248 0.0.0.7 area 0
!
ip classless
!
!
```

- El router Centro necesita configurar OSPF, la publicación de las subredes de las interfaces serial 0/1 (enlace con router SUR) y FastEthernet 0/0 (red Lan). Asimismo, se requiere de una ruta por defecto para alcanzar Internet.

```
CENTRO#SH RUN
!
!
!
interface Loopback0
 ip address 208.8.8.8 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 172.16.8.2 255.255.255.252
 !
interface Serial0/1
 ip address 192.168.1.254 255.255.255.248
 clock rate 64000
!
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.1.248 0.0.0.7 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!
```

- Para el router ISP sólo requiere de una configuración básica. Se le añadió una interfaz loopback y una conexión en su interfaz FastEthernet para la representación de servidores de Internet.

```
ISP#sh run
!
!
!
interface Loopback0
 ip address 209.89.9.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 208.23.78.45 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.16.8.1 255.255.255.252
 clock rate 64000
!
!
```

FASE 2: DIAGNÓSTICO DE ENRUTAMIENTO:

- **TABLA DE VECINOS EN ROUTERS SUR Y CENTRO:**

```
SUR#SH IP OSPF NEIghbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
208.8.8.8         0   FULL/  -        00:00:39    192.168.1.254   Serial0/0
```

```
CENTRO#SH IP OSPF NEighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
209.9.9.9         0   FULL/  -        00:00:36    192.168.1.253   Serial0/1
CENTRO#
```

- **TABLA DE ENRUTAMIENTO:**

```
SUR# SH IP ROUTE
Gateway of last resort is 192.168.1.254 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.1.0/27 [110/65] via 192.168.1.254, 00:20:59, Serial0/0
C       192.168.1.32/27 is directly connected, FastEthernet0/0
C       192.168.1.248/29 is directly connected, Serial0/0
    209.9.9.0/32 is subnetted, 1 subnets
C       209.9.9.9 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.254, 00:20:59, Serial0/0
```

```
CENTRO#SH IP ROUTE
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.16.0.0/30 is subnetted, 1 subnets
C       172.16.8.0 is directly connected, Serial0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/27 is directly connected, FastEthernet0/0
C       192.168.1.248/29 is directly connected, Serial0/1
    208.8.8.0/32 is subnetted, 1 subnets
C       208.8.8.8 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Serial0/0
```

```
ISP#sh ip route
Gateway of last resort is not set
    172.16.0.0/30 is subnetted, 1 subnets
C       172.16.8.0 is directly connected, Serial0/0
C    208.23.78.0/24 is directly connected, FastEthernet0/1
    209.89.9.0/32 is subnetted, 1 subnets
C       209.89.9.1 is directly connected, Loopback0
```

FASE 3: CONFIGURACIÓN DE NAT DINÁMICO – ROUTER SUR:

- Como es conocido, el NAT DINÁMICO permite la traducción de direcciones de forma aleatoria hacia un rango de direcciones.
- En este caso, las direcciones de la subred incluidas en la **lista de acceso 20** serán traducidas a las direcciones del pool **prueba**.
- La interfaz FastEthernet 0/0 será la entrada del servicio NAT y la interfaz serial 0/0, la salida.

```
SUR#SH RUN
!
!
interface Loopback0
 ip address 209.9.9.9 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.33 255.255.255.224
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 192.168.1.253 255.255.255.248
 ip nat outside
!
!
router ospf 1
 log-adjacency-changes
```

```
 network 172.17.1.0 0.0.0.15 area 0
 network 192.168.1.248 0.0.0.7 area 0
!
ip nat pool prueba 192.168.1.249 192.168.1.251 netmask 255.255.255.248
ip nat inside source list 20 pool prueba
ip classless
!
!
access-list 20 permit 192.168.1.32 0.0.0.31
!
!
```

- Se verifica a través de la tabla de NAT el proceso de traducción, donde los Hosts de la red Lan del router Sur prueban conectividad hacia la red Lan del router Centro, así como el acceso al router.
- Obsérvese que al Host 192.168.1.35 se le asigna la dirección 192.168.1.250 siempre que realiza la prueba a diferentes Hosts; asimismo, al Host 192.168.1.36 se le asigna la dirección 192.168.1.249.

```
SUR#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.1.250:21 192.168.1.35:21    192.168.1.2:21     192.168.1.2:21
icmp 192.168.1.250:22 192.168.1.35:22    192.168.1.2:22     192.168.1.2:22
icmp 192.168.1.250:25 192.168.1.35:25    192.168.1.3:25     192.168.1.3:25
icmp 192.168.1.250:26 192.168.1.35:26    192.168.1.3:26     192.168.1.3:26
icmp 192.168.1.249:17 192.168.1.36:17    192.168.1.254:17   192.168.1.254:17
icmp 192.168.1.249:18 192.168.1.36:18    192.168.1.254:18   192.168.1.254:18
icmp 192.168.1.249:19 192.168.1.36:19    192.168.1.2:19     192.168.1.2:19
icmp 192.168.1.249:20 192.168.1.36:20    192.168.1.2:20     192.168.1.2:20
icmp 192.168.1.249:21 192.168.1.36:21    192.168.1.2:21     192.168.1.2:21
icmp 192.168.1.249:22 192.168.1.36:22    192.168.1.2:22     192.168.1.2:22
icmp 192.168.1.249:23 192.168.1.36:23    192.168.1.3:23     192.168.1.3:23
icmp 192.168.1.249:24 192.168.1.36:24    192.168.1.3:24     192.168.1.3:24
```

FASE 4: CONFIGURACIÓN DE NAT DE SOBRECARGA (PAT) – ROUTER NORTE:

- El NAT DE SOBRECARGA (PAT) permite la traducción de direcciones hacia una dirección, con la diferencia de que varía el número de puerto. Puede definirse un rango de direcciones.
- En este caso, las direcciones de la subred incluidas en la **lista de acceso 30** serán traducidas a la dirección de la interfaz serial 0/0 (192.168.1.254).
- La interfaz FastEthernet 0/0 y la interfaz serial 0/1 serán la entrada del servicio PAT y la interfaz serial 0/0, la salida.

```
CENTRO#SH RUN
!
!
!
interface Loopback0
 ip address 208.8.8.8 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
 ip nat inside
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 172.16.8.2 255.255.255.252
 ip nat outside
!
interface Serial0/1
 ip address 192.168.1.254 255.255.255.248
 ip nat inside
 clock rate 64000
!
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.1.248 0.0.0.7 area 0
 default-information originate
!
ip nat inside source list 30 interface Serial0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!
access-list 30 permit 192.168.1.0 0.0.0.255
!
!
```

- Se verifica a través de la tabla de NAT el proceso de traducción, donde se realizan pruebas hasta los puntos de Internet.
- Deben realizarse pruebas desde tres lugares: los Hosts de la Lan del router Sur, los Hosts de la red Lan del router Centro y desde el router SUR. Si se desea realizar la prueba desde el router Centro no se observaría la diferencia ya que emplearía su propia interfaz serial 0/0, lo cual podríamos solucionar con un ping extendido y usando la otra dirección IP.
- **PRUEBA DESDE LOS HOSTS DE LA LAN DE CENTRO**:
  - Al realizar las pruebas desde la red Lan del router Centro hacia Internet, se verifica la traducción empleando la misma dirección pero con diferente puerto.
  - Primero el Host 192.168.1.2 y luego el Host 192.168.1.3.

```
CENTRO#clear ip nat translation *
CENTRO#SH IP NAT TRAnslations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 172.16.8.2:10     192.168.1.2:10     208.23.78.46:10    208.23.78.46:10
icmp 172.16.8.2:11     192.168.1.2:11     208.23.78.46:11    208.23.78.46:11
icmp 172.16.8.2:12     192.168.1.2:12     209.89.9.1:12      209.89.9.1:12
icmp 172.16.8.2:13     192.168.1.2:13     209.89.9.1:13      209.89.9.1:13
icmp 172.16.8.2:14     192.168.1.2:14     209.89.9.1:14      209.89.9.1:14
icmp 172.16.8.2:15     192.168.1.2:15     209.89.9.1:15      209.89.9.1:15
icmp 172.16.8.2:8      192.168.1.2:8      208.23.78.46:8     208.23.78.46:8
icmp 172.16.8.2:9      192.168.1.2:9      208.23.78.46:9     208.23.78.46:9
tcp 172.16.8.2:1034    192.168.1.2:1034   172.16.8.1:23      172.16.8.1:23
```

```
CENTRO#SH IP NAT TRAnslations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 172.16.8.2:10     192.168.1.3:10     209.89.9.1:10      209.89.9.1:10
icmp 172.16.8.2:11     192.168.1.3:11     209.89.9.1:11      209.89.9.1:11
icmp 172.16.8.2:12     192.168.1.3:12     209.89.9.1:12      209.89.9.1:12
icmp 172.16.8.2:5      192.168.1.3:5      172.16.8.1:5       172.16.8.1:5
icmp 172.16.8.2:6      192.168.1.3:6      172.16.8.1:6       172.16.8.1:6
icmp 172.16.8.2:7      192.168.1.3:7      172.16.8.1:7       172.16.8.1:7
icmp 172.16.8.2:8      192.168.1.3:8      172.16.8.1:8       172.16.8.1:8
icmp 172.16.8.2:9      192.168.1.3:9      209.89.9.1:9       209.89.9.1:9
tcp 172.16.8.2:1025    192.168.1.3:1025   172.16.8.1:23      172.16.8.1:23
```

- **PRUEBA DESDE LOS HOSTS DE LA LAN DE SUR**:
  - Al realizar las pruebas de conectividad, Telnet o acceso web, comprobamos que al Host 192.168.1.36 se le asigna a través del NAT, en router Sur, la dirección 192.168.1.250 y posteriormente, en el servicio PAT, en router CENTRO, se le asigna el IP 172.16.8.2 con diferente número de puerto.
  - En el caso del Host 192.168.1.35, se le asigna a través del NAT, en router Sur, la dirección 192.168.1.251 y posteriormente, en el servicio PAT, en router CENTRO, se le asigna el IP 172.16.8.2 con diferente número de puerto.

```
SUR#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.1.250:31  192.168.1.36:31    209.89.9.1:31      209.89.9.1:31
icmp 192.168.1.250:32  192.168.1.36:32    209.89.9.1:32      209.89.9.1:32
icmp 192.168.1.250:33  192.168.1.36:33    209.89.9.1:33      209.89.9.1:33
icmp 192.168.1.250:34  192.168.1.36:34    209.89.9.1:34      209.89.9.1:34
tcp 192.168.1.251:1025 192.168.1.35:1025  208.23.78.46:80    208.23.78.46:80
tcp 192.168.1.251:1026 192.168.1.35:1026  208.23.78.46:80    208.23.78.46:80
tcp 192.168.1.251:1027 192.168.1.35:1027  208.23.78.46:23    208.23.78.46:23
tcp 192.168.1.250:1026 192.168.1.36:1026  172.16.8.1:23      172.16.8.1:23
```

```
CENTRO#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 172.16.8.2:31     192.168.1.250:31   209.89.9.1:31      209.89.9.1:31
icmp 172.16.8.2:32     192.168.1.250:32   209.89.9.1:32      209.89.9.1:32
icmp 172.16.8.2:33     192.168.1.250:33   209.89.9.1:33      209.89.9.1:33
icmp 172.16.8.2:34     192.168.1.250:34   209.89.9.1:34      209.89.9.1:34
tcp 172.16.8.2:1024    192.168.1.250:1026 172.16.8.1:23      172.16.8.1:23
tcp 172.16.8.2:1025    192.168.1.251:1025 208.23.78.46:80    208.23.78.46:80
tcp 172.16.8.2:1026    192.168.1.251:1026 208.23.78.46:80    208.23.78.46:80
tcp 172.16.8.2:1027    192.168.1.251:1027 208.23.78.46:23    208.23.78.46:23
```

CONCLUSIONES Y/U OBSERVACIONES

_____

_____

_____

LABORATORIO N° 4 - TOPOLOGÍA HUB AND SPOKE CON SPLIT HORIZON

INTRODUCCIÓN

Rara vez se encuentra una topología punto a punto sobre dos únicas ubicaciones donde configurar Frame Relay. En la mayoría de las ocasiones, la topología utilizada es una de las siguientes:

- **Topología en estrella**. También conocida como hub-and-Spoke. Es la más popular y la menos cara, ya que requiere del menor número de PVC. El router central suministra una conexión multipunto, utilizando una única interfaz individual para interconectar múltiples PVC.
- **Topología en malla completa**. Todos los routers tienen circuitos virtuales al resto de los destinos. Es muy costosa pero soporta redundancia.
- **Topología en malla parcial**. En ésta, no todos los sitios tienen acceso directo al resto de sitios.

  Para hacer funcionar una interfaz Frame Relay como multipunto podemos configurarla como tal o como varias subinterfaces punto a punto. En todos los casos, Frame Relay utiliza el DLCI para distinguir entre los distintos circuitos virtuales de la red Frame Relay.

OBJETIVOS

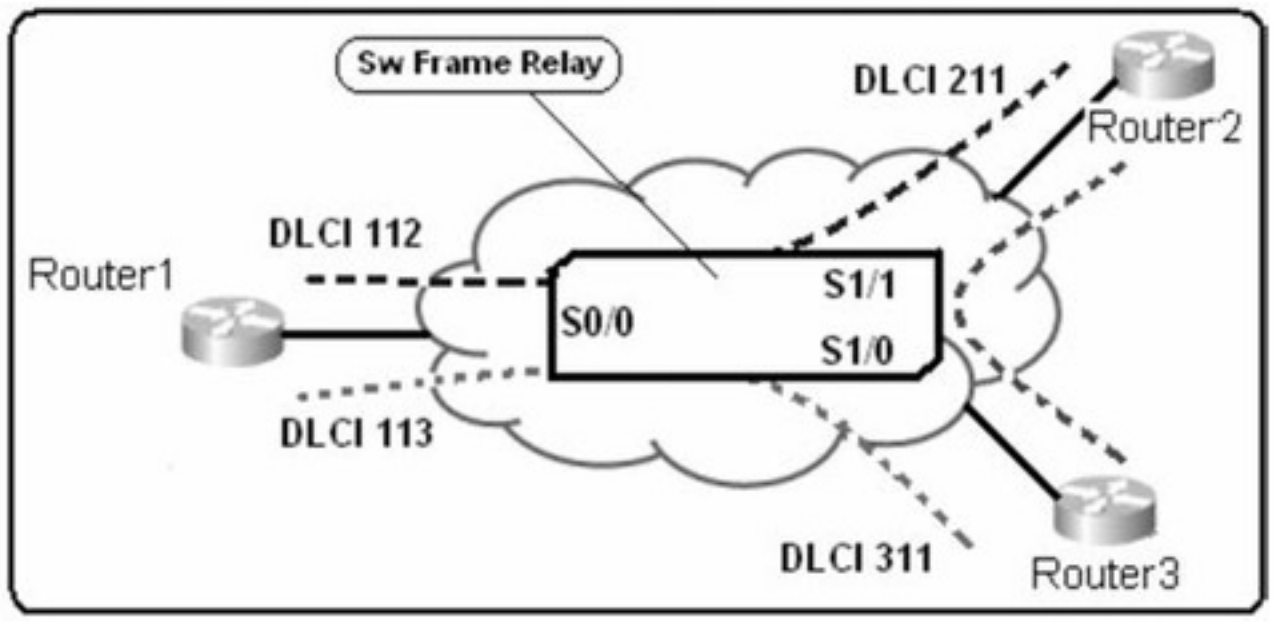
- Configuración de un router Cisco como un switch Frame Relay.
- Implementación del enrutamiento EIGRP sobre una la topología **hub and Spoke**.

PROCEDIMIENTO

La implementación de la red planteada está basada en una red hub and Spoke para ser desarrollada de acuerdo a la situación de los casos planteados.

Para el primer caso se desarrolla la implementación del switch Frame Relay que servirá de base para las siguientes implementaciones. El segundo caso plantea el uso de interfaces físicas y el caso tres, el uso de sub-interfaces. Los dos últimos casos están desarrollados con el protocolo de enrutamiento EIGRP.

DESARROLLO



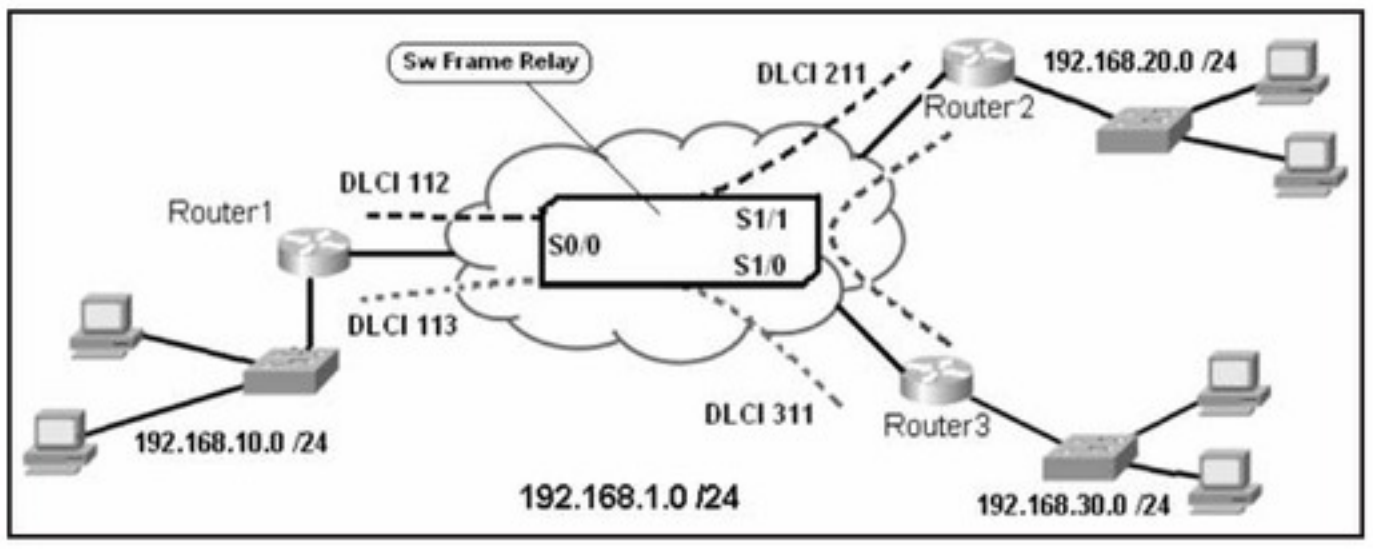
1. Verifique el estado del router.
2. Si lo requiere el caso, elimine la configuración de cada router y reinícielo.
3. Habilite la opción de captura de texto en el Hyperterminal.
4. Realice la configuración básica de cada router con ayuda del bloc de notas.

CASO 1: Configuración del switch Frame Relay

1. Se deberá realizar la siguiente configuración en un router para permitir su operación como switch Frame Relay.
2. Al completar esta configuración permitirá que se enrute la información de la interfaz serial 0/0 hacia la interfaz serial 1/1 (DLCI 112 al DLCI 211), y de la interfaz serial 0/0 hacia la interfaz serial 1/0 (DLCI 113 al DLCI 311), pero no podrá transmitirse desde la interfaz serial 1/1 hacia la interfaz serial 1/0.

```
FR#configure terminal
FR(config)#frame-relay switching
FR(config)#interface s0/0
FR(config-if)#no ip address
FR(config-if)#encapsulation frame-relay
FR(config-if)#clock rate 64000
FR(config-if)#frame-relay intf-type ansi
FR(config-if)#frame-relay route 112 interface serial 1/1 211
FR(config-if)#frame-relay route 113 interface serial 1/0 311
FR(config-if)#no shutdown
FR(config-if)#interface s1/0
FR(config-if)#no ip address
FR(config-if)#encapsulation frame-relay
FR(config-if)#clock rate 64000
FR(config-if)#frame-relay intf-type ansi
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay route 311 interface serial 0/0 113
FR(config-if)#no shutdown
FR(config-if)#interface s1/1
FR(config-if)#no ip address
FR(config-if)#encapsulation frame-relay
FR(config-if)#clock rate 64000
FR(config-if)#frame-relay intf-type ansi
FR(config-if)#frame-relay route 211 interface serial 0/0 112
FR(config-if)#no shutdown
```

CASO 2: Implementación mediante interfaces



1. En cada router se deberá habilitar el encapsulamiento Frame Relay y asignar su dirección IP, como se indica para cada uno:

```
LIMA#configure terminal
LIMA(config)#interface s0/0
LIMA(config-if)#encapsulation frame-relay
LIMA(config-if)#ip address 192.168.1.1 255.255.255.0
LIMA(config-if)#no shutdown
```

```
CUZCO#configure terminal
CUZCO(config)#interface s0/0
CUZCO(config-if)#encapsulation frame-relay
CUZCO(config-if)#ip address 192.168.1.2 255.255.255.0
CUZCO(config-if)#no shutdown
```

```
AREQUIPA#configure terminal
AREQUIPA(config)#interface s0/0
AREQUIPA(config-if)#encapsulation frame-relay
AREQUIPA(config-if)#ip address 192.168.1.3 255.255.255.0
AREQUIPA(config-if)#no shutdown
```

2. Habilitar el enrutamiento EIGRP en cada router dentro del AS 64500, donde deberán identificarse los vecinos EIGRP previamente configurados.

```
LIMA(config)#interface Serial0/0
LIMA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
LIMA(config-if)#encapsulation frame-relay
LIMA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
LIMA(config-if)#exit
LIMA(config)#router eigrp 64500
LIMA(config-router)#no auto
LIMA(config-router)#net 192.168.1.0
LIMA(config-router)#net 192.168.10.0
%DUAL-5-NBRCHANGE: IP-EIGRP 64500: Neighbor 192.168.1.2 (Serial0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 64500: Neighbor 192.168.1.3 (Serial0/0) is up: new adjacency
LIMA(config-router)#
```

3. Se realiza el diagnóstico en cada router sobre la publicación de redes con ayuda de la tabla de enrutamiento.

```
LIMA#show ip route
Gateway of last resort is not set
    192.168.1.0/29 is subnetted, 1 subnets
C      192.168.1.0 is directly connected, Serial0/0
C   192.168.10.0/24 is directly connected, FastEthernet0/0
D   192.168.20.0/24 [90/2172416] via 192.168.1.3, 00:07:30, Serial0/0
D   192.168.30.0/24 [90/2172416] via 192.168.1.2, 00:07:31, Serial0/0
```

```
CUZCO#show ip route
Gateway of last resort is not set
    192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
D    192.168.10.0/24 [90/2172416] via 192.168.1.1, 00:12:30, Serial0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
CUZCO#
```

```
AREQUIPA#show ip route
Gateway of last resort is not set
    192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
D    192.168.10.0/24 [90/2172416] via 192.168.1.1, 00:13:56, Serial0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
AREQUIPA#
```

4. Configure cada estación de trabajo conectada a los routers Lima, Cuzco y Arequipa.
5. Verifique que cada red no conectada directamente se encuentre listada en la tabla de enrutamiento que se presenta.
6. Borrando el mapa Frame Relay **Clear frame-relay inarp**.

```
CUZCO#clear frame-relay inarp
%DUAL-5-NBRCHANGE: IP-EIGRP 64500: Neighbor 192.168.1.1 (Serial0/0) is down: holding time expired
CUZCO#show ip route
Gateway of last resort is not set
    192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
CUZCO#
%DUAL-5-NBRCHANGE: IP-EIGRP 64500: Neighbor 192.168.1.1 (Serial0/0) is up: new adjacency

CUZCO#show ip route
Gateway of last resort is not set
    192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
D    192.168.10.0/24 [90/2172416] via 192.168.1.1, 00:00:19, Serial0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
CUZCO#
```

7. Realice las pruebas de conectividad necesarias con el comando **PING** hacia todos los Hosts y routers de la topología de red.
   - Si el ping no es exitoso verifique el posible problema.

```
C:\Users\hector>ping 192.168.20.1
Haciendo ping a 192.168.20.1 con 32 bytes de datos:
Respuesta desde 192.168.20.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.20.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.1: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.20.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

```
C:\Users\hector>ping 192.168.30.1
Haciendo ping a 192.168.30.1 con 32 bytes de datos:
Respuesta desde 192.168.30.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.30.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.30.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.30.1: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.30.1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

```
C:\Users\DAGO>ping 192.168.10.1
Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.10.1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 0ms, Máximo = 2ms, Media = 0ms
C:\Users\DAGO>ping 192.168.20.1
Haciendo ping a 192.168.20.1 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 192.168.20.1:
   Paquetes: enviados = 4, recibidos = 0, perdidos = 4
   (100% perdidos),
```

8. Para que enrute entre R2 y R3, habilite un DLCI entre ambos; en el switch Frame Relay configure:
   a. Interfaz Serial 1/0
      i. **frame-relay route 312 interface serial 213**
   b. Interfaz Serial 1/1
      i. **frame-relay route 213 interface serial 312**

CASO 3: Implementación mediante subinterfaces:

Cuando una interfaz individual debe interconectar múltiples sitios, pueden surgir problemas de accesibilidad derivados del carácter de multiacceso sin difusión (NBMA) de Frame Relay. Las interfaces Frame Relay utilizan el algoritmo de **Horizonte Dividido** (split horizon) para reducir el número de bucles de enrutamiento. En virtud de dicho algoritmo no se permite que una actualización de enrutamiento recibida sobre una interfaz sea enviada a la misma interfaz.

Como resultado, si un router remoto envía una actualización de enrutamiento al router central, éste no puede enviar esa difusión a través de la misma interfaz a los otros routers remotos, aunque utilicen PVC separados (ya que están en la misma interfaz).

Otro problema sería considerar el ancho de banda consumido por las actualizaciones de enrutamiento, el protocolo CDP, etc. La solución a este problema es la utilización de **subinterfaces**, ya que las actualizaciones

de enrutamiento recibidas por una subinterfaz sí pueden ser enviadas por otra subinterfaz. Pueden configurarse las subinterfaces para que soporten conexiones punto a punto (un DLCI, una subred) y multipunto (múltiples DLCI, una subred).

- **Configuración de dos subinterfaces punto a punto:**

```
Interface serial0
No ipaddress
Encapsulation frame-relay
Interface serial0.2 point-to-point
Ip address 192.168.0.1 255.255.255.0
Bandwidth 64
Frame-relay interface-dlci 110
Interface serial0.3 point-to-point
Ip address 192.168.1.1 255.255.255.0
Bandwidth 64
Frame-relay interface dlci 120
```

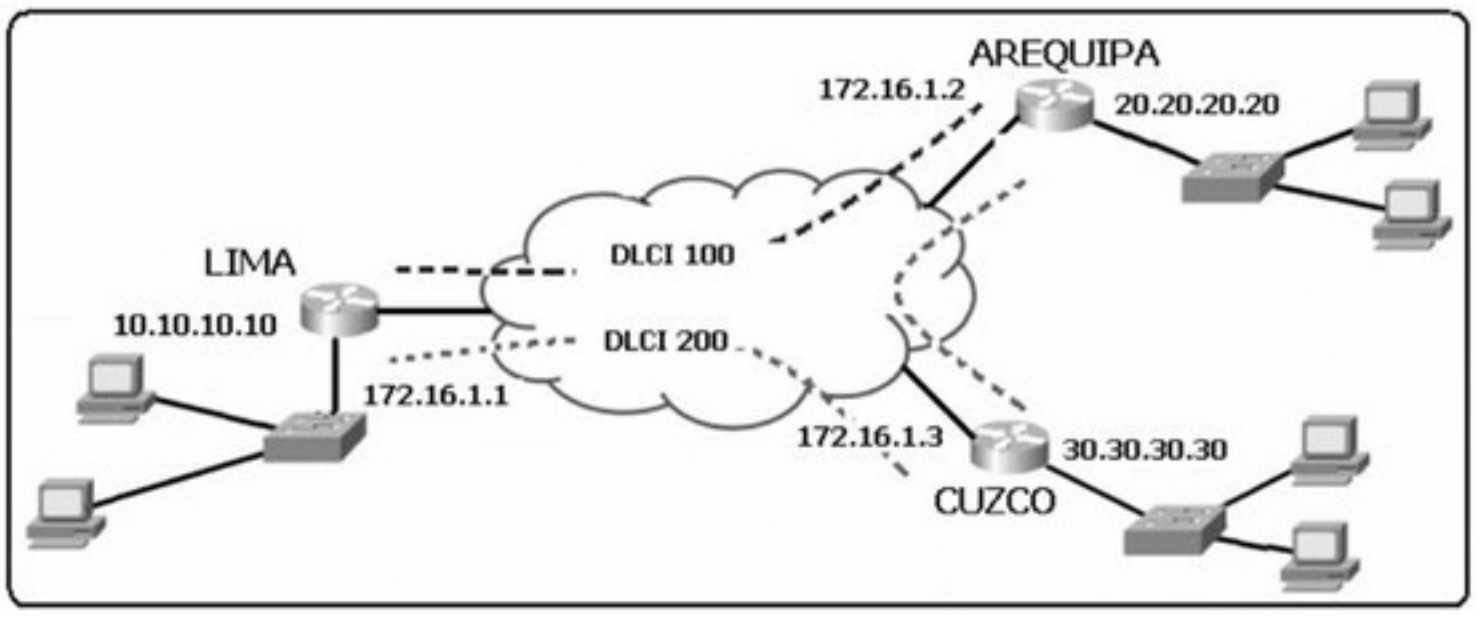
- **Configurar una subinterfaz multipunto:**

```
Interface Serial2
No ip address
Encapsulation frame-relay
No inverse-arp
Interface serial2.2 multipoint
Ip address 192.168.0.1 255.255.255.0
Bandwidth 64
Frame-relay map ip 192.168.0.2 120 broadcast
Frame-relay map ip 192.168.0.3 130 broadcast
Frame-relay map ip 192.168.0.4 140 broadcast
```

DESARROLLO:

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

1. **CONFIGURACIÓN BÁSICA**:
   a. Realizar las conexiones y eliminar la configuración de cada router, en caso la tenga.
   b. Habilite la opción de captura de texto en el Hyperterminal.
   c. Realice la configuración básica con ayuda del editor de texto.



2. ENCAPSULAMIENTO FRAME RELAY

- De forma similar a los casos presentados como ejemplo, se implementa la configuración de los equipos.
- El router Lima, como se observa, habilitará una subinterfaz en modo multipunto, estableciendo un mapeo hacia cada dirección IP de sus routers vecinos mediante el DLCI correspondiente.

```
hostname LIMA
!
interface Loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Serial0
bandwidth 128
no ip address
encapsulation frame-relay
no ip mroute-cache
no fair-queue
no frame-relay inverse-arp
frame-relay lmi-type cisco
!
interface Serial0.1 multipoint
description Frame Relay DLCI 100 (AREQUIPA) y 200 (CUZCO)
ip address 172.16.1.1255.255.255.0
frame-relay map ip 172.16.1.2 100 broadcast
frame-relay map ip 172.16.1.3 200 broadcast
!
router eigrp 200
passive-interface Loopback0
network 10.10.10.10 0.0.0.0
network 172.16.1.1 0.0.0.0
no auto-summary
```

- La configuración de los routers Arequipa y Cuzco requieren de un encapsulamiento Frame Relay y del mapeo hacia la dirección del router Lima con su respectiva DLCI.

```
hostname AREQUIPA
!
interface Loopback0
ip address 20.20.20.20  255.255.255.255
no ip directed-broadcast
!
interface Serial0/0
ip address 172.16.1.2 255.255.255.0
no ip directed-broadcast
encapsulation frame-relay
frame-relay map ip 172.16.1.1 100 broadcast
no frame-relay inverse-arp
!
router eigrp 200
passive-interface Loopback0
network 20.20.20.20  0.0.0.0
network 172.16.1.2 0.0.0.0
no auto-summary
```

```
hostname CUZCO
!
interface Loopback0
ip address 30.30.30.30  255.255.255.255
!
interface Serial0/0
ip address 172.16.1.3 255.255.255.0
encapsulation frame-relay
frame-relay map ip 172.16.1.1 200 broadcast
no frame-relay inverse-arp
!
router eigrp 200
passive-interface Loopback0
network 30.30.30.30  0.0.0.0
network 172.16.1.3 0.0.0.0
no auto-summary
no eigrp log-neighbor-changes
```

3. **HORIZONTE DIVIDIDO**

- Al revisar la tabla de enrutamiento en Arequipa se puede observar que se están aprendiendo solas las rutas por EIGRP, originadas en LIMA, y no las originadas en CUZCO (30.30.30.30 /32).

```
AREQUIPA#sh ip rou
……..<resultado omitido>……
Gateway of last resort is not set

20.0.0.0/32 is subnetted, 1 subnets
C       20.20.20.20  is directly connected, Loopback0
172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.10.10.10/32 [90/2297856] via 172.31.1.3, 00:12:37, Serial0/0
C       10.1.1.0/24 is directly connected, FastEthernet0/0
C       10.1.0.0/24 is directly connected, FastEthernet0/1
C       10.1.5.0/24 is directly connected, Loopback1
AREQUIPA#
```

- La situación anterior es síntoma de la regla básica en los protocolos de enrutamiento Vector Distancia: la regla del horizonte dividido (*Split Horizon*). Por lo tanto, habría que deshabilitar en Lima con el comando ip split-horizon. Pero para el caso específico del protocolo EIGRP, esto deberá realizarse como se muestra en el ejemplo.

```
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#int s0.1
LIMA(config-subif)#ip split-horizon
LIMA(config-subif)#no ip split-horizon eigrp 200
LIMA(config-subif)#
*Mar 16 21:44:46.045: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.1.2 (Serial0.1) is down:
split horizon changed
*Mar 16 21:44:46.045: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.1.3 (Serial0.1) is down:
split horizon changed
LIMA(config-subif)#
```

- Si trabaja con el protocolo RIP utilice el mismo comando pero de la siguiente forma:

```
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#int s0.1
LIMA(config-subif)#no ip split-horizon
LIMA(config-subif)#end
LIMA#
```

- Se verifica en el router Arequipa, luego de unos segundos, que se aprenden todas las rutas.

```
AREQUIPA#sh ip rou
……..<resultado omitido>……
Gateway of last resort is not set

20.0.0.0/32 is subnetted, 1 subnets
C       20.20.20.20  is directly connected, Loopback0
30.0.0.0/32 is subnetted, 1 subnets
D       30.30.30.30  [90/2809856] via 172.31.1.3, 00:06:00, Serial0/0
172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.10.10.10/32 [90/2297856] via 172.31.1.3, 00:06:00, Serial0/0
C       10.1.1.0/24 is directly connected, FastEthernet0/0
C       10.1.0.0/24 is directly connected, FastEthernet0/1
C       10.1.5.0/24 is directly connected, Loopback1
AREQUIPA#
```

4. DIAGNÓSTICO

- Si se prueba la conectividad, no funcionará.

```
AREQUIPA#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30 , timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
AREQUIPA#
```

- Verificando, se descarta: el destino está efectivamente en la tabla de enrutamiento de Arequipa y el mapeo del next hop está correcto a nivel de Frame Relay, según indica el comando show frame-relay map.

```
AREQUIPA#sh ip route 30.30.30.30
Routing entry for 30.30.30.30 /32
Known via “eigrp 200”, distance 90, metric 2809856, type internal
Redistributing via eigrp 200
Last update from 172.16.1.1on Serial0/0, 04:30:50 ago
Routing Descriptor Blocks:
* 172.16.1.1, from 172.16.1.1, 04:30:50 ago, via Serial0/0
 Route metric is 2809856, traffic share count is 1
 Total delay is 45000 microseconds, minimum bandwidth is 1544 Kbit
 Reliability 255/255, minimum MTU 1500 bytes
 Loading 3/255, Hops 2
AREQUIPA#
```

```
AREQUIPA#sh frame-relay map
Serial0/0 (up): ip 172.16.1.1DLCI 100(0x6F,0x18F0), static,
        broadcast,
        CISCO, status defined, active
AREQUIPA#
```

- El análisis desde Cuzco mostrará qué es lo que está faltando. El ping es generado por la interfaz s0/0 de Arequipa, así que la respuesta desde Cuzco es destinada a 172.16.1.2.

```
CUZCO#sh ip rou 172.31.1.1
Routing entry for 172.16.1.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Redistributing via eigrp 200
Routing Descriptor Blocks:
* directly connected, via Serial0/0
 Route metric is 0, traffic share count is 1
```

```
CUZCO#sh frame-relay map
Serial0/0 (up): ip 172.16.1.1DLCI 200(0x70,0x1C00), static,
        broadcast,
        CISCO, status defined, active
CUZCO#
```

- El destino aparece en la tabla de enrutamiento, sin embargo, Frame Relay no sabe qué DLCI utilizar para transportar el frame. Esto se configura con el comando frame-relay map. Una forma automática de obtener estos valores es utilizando el comando frame-relay inverse-arp, sin embargo, no permite llevar el control completo de la red.

```
CUZCO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUZCO(config)#interface Serial0/0
CUZCO(config-if)#frame-relay map ip 172.16.1.2 200 broadcast
CUZCO(config-if)#^Z
CUZCO#
```

- Con esto se soluciona el inconveniente:

```
AREQUIPA#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/46/52 ms
AREQUIPA#
```

TAREA

- Implementar la comunicación del circuito mediante subinterfaces, con la opción punto a punto.
- A continuación se añade la configuración necesaria.

1. Activar las subinterfaces punto a punto en cada router.

```
LIMA#configure terminal
LIMA(config)#interface s0/0
LIMA(config-if)#no shutdown
LIMA(config-if)#encapsulation frame-relay
LIMA(config)#interface s0/0.1 point to point
LIMA(config-if)#ip address 192.168.10.1 255.255.255.0
LIMA(config-if)#frame-relay interface dlci 112
LIMA(config)#interface s0/0.2 point to point
LIMA(config-if)#ip address 192.168.20.1 255.255.255.0
LIMA(config-if)#frame-relay interface dlci 113
```

```
CUZCO#configure terminal
CUZCO(config)#interface s0/0
CUZCO(config-if)#encapsulation frame-relay
CUZCO(config-if)#no shutdown
CUZCO(config)#interface s0/0.1 point to point
CUZCO(config-if)#ip address 192.168.10.2 255.255.255.0
CUZCO(config-if)#frame-relay interface dlci 211
```

```
AREQUIPA#configure terminal
AREQUIPA(config)#interface s0/0
AREQUIPA(config-if)#encapsulation frame-relay
AREQUIPA(config-if)#no shutdown
AREQUIPA(config)#interface s0/0.1 point to point
AREQUIPA(config-if)#ip address 192.168.20.2 255.255.255.0
AREQUIPA(config-if)# frame-relay interface dlci 311
```

CONCLUSIONES Y/U OBSERVACIONES

_____

_____

_____

LABORATORIO N° 5 - Topología NBMA

INTRODUCCIÓN

Las redes NBMA soportan varios routers pero no son de difusión, por lo que podrían surgir problemas de alcance. En el caso de comunicar una topología en malla o punto – multipunto, no se garantiza que los demás routers reciban difusiones, por lo que, si se desea garantizar esto, habrá que activarlo en los circuitos virtuales.

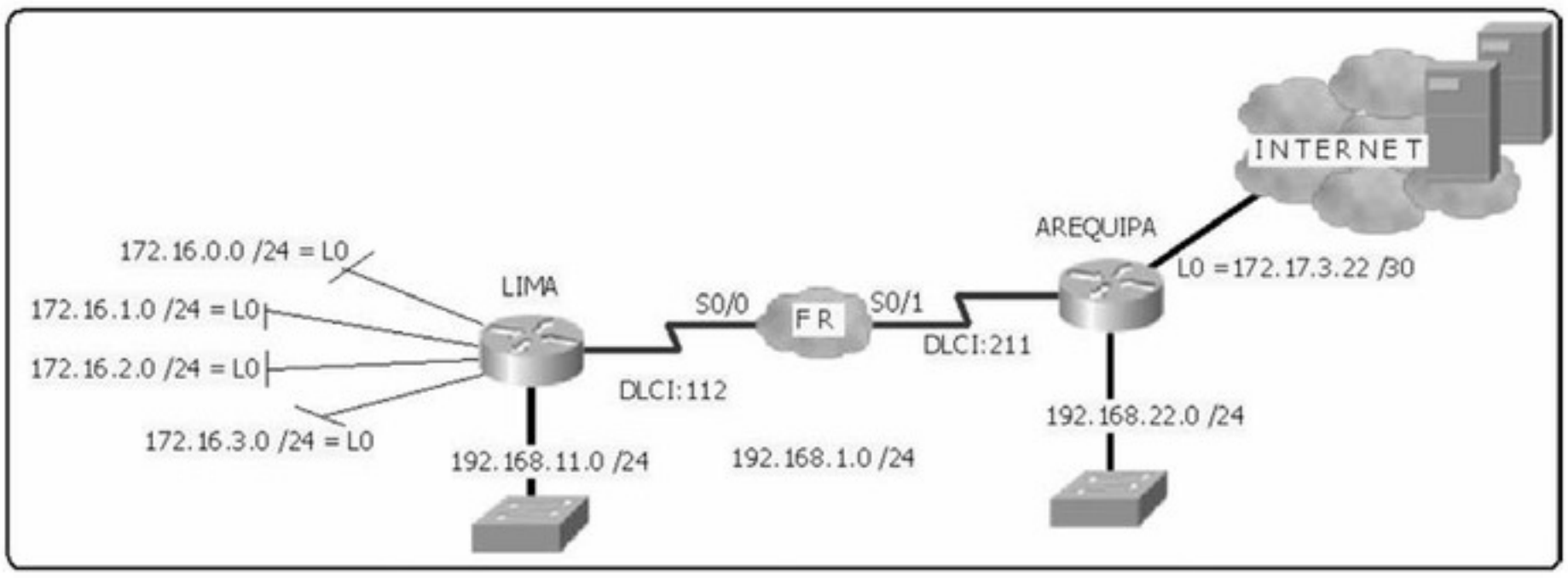
OBJETIVOS

- Configuración de router Cisco como un switch Frame Relay.
- Implementación del enrutamiento EIGRP, OSPF Y RIP sobre una nube Frame Relay.

DESCRIPCIÓN

La implementación del circuito es una conexión virtual mediante el encapsulamiento Frame Relay, empleando un router Cisco como switch Frame Relay. La configuración del laboratorio puede permitirle una conexión NBMA en malla, malla parcial o punto a punto, dependiendo del protocolo.

Se desarrolla en cuatro secciones denominadas casos, en los cuales se trabaja con protocolos RIP, EIGRP y OSPF.



DESARROLLO

Tener en cuenta que se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo con ayuda de laboratorios anteriores.

- En este caso se colocará una interfaz loopback representando a la conexión a Internet y su ruta por defecto direccionada tendrá salida a dicha interfaz.

CASO I: CONFIGURACIÓN BÁSICA DEL SWITCH FR Y ROUTER

1. CONFIGURACIÓN BÁSICA:
   a. Realice las conexiones y elimine la configuración de cada router, en caso la tenga.
   b. Habilite la opción de captura de texto en el Hyperterminal.
   c. Realice la configuración básica con ayuda del editor de texto.

2. **CONFIGURANDO EL SWITCH FRAME RELAY**:
   - Se debe verificar si las interfaces de los routers están activadas.

```
SW-FR#sh protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
Serial0/0 is up, line protocol is up
Serial0/1 is up, line protocol is up
```

   - Se identifican los equipos vecinos con ayuda del protocolo CDP.

```
SW-FR#sh cdp n
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
AREQUIPA       Ser 0/1          170        R           1760      Ser 0/1
LIMA           Ser 0/0          175        R S         1760      Ser 0/0
```

   - Se procede a la habilitación del router como switch Frame Relay. Para los casos a configurar podría habilitar otras interfaces con DLCI y establecer la conexión con un mayor número de routers.

```
SW-FR#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-FR(config)#frame-relay switching
SW-FR(config)#int S0/0
SW-FR(config-if)#encapsulation frame-relay
SW-FR(config-if)#frame-relay lmi-type ansi
SW-FR(config-if)#frame-relay intf-type dce
SW-FR(config-if)#frame-relay route 112 interface s0/1 211
*Jul  1 05:48:41.916: %SYS-5-CONFIG_I: Configured from console by console
*Jul  1 05:48:42.429: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
SW-FR(config-if)#exit
SW-FR(config)#int s0/1
SW-FR(config-if)#encapsulation frame-relay
SW-FR(config-if)#frame-relay intf-type dce
SW-FR(config-if)#frame-relay lmi-type ansi
*Jul  1 05:09:28.149: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to
down
SW-FR(config-if)#frame-relay route 211 interface s0/0 112
SW-FR(config-if)#^Z
SW-FR#wr
Building configuration...
*Jul  1 05:09:58.379: %SYS-5-CONFIG_I: Configured from console by console
```

3. **CONFIGURACIÓN FR DEL ROUTER AREQUIPA**:

- Se comprueba que la interfaz serial 0/1 estará desactivada a raíz del encapsulamiento HDLC.

```
AREQUIPA#sh protocols
Global values:
 Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
Serial0/0 is administratively down, line protocol is down
Serial0/1 up, line protocol is down
```

- Encapsulamiento Frame Relay.

a. Al habilitar el encapsulamiento se muestra un mensaje indicando que la interfaz serial 0/1 está activa.

```
AREQUIPA(config)#INT S0/1
AREQUIPA(config-if)#ENcapsulation FRame-relay
AREQUIPA(config-if)#IP ADD 192.168.10.2 255.255.255.0
*Mar  1 00:27:37.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
AREQUIPA(config-if)#NO SHUT
AREQUIPA(config-if)#^Z
AREQUIPA#CONF T
*Mar  1 00:27:57.285: %SYS-5-CONFIG_I: Configured from console by console
```

b. Se comprueba el estado de la interfaz:

```
AREQUIPA#show protocols
Global values:
 Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
Serial0/0 is administratively down, line protocol is down
Serial0/1 is up, line protocol is up
  Internet address is 192.168.10.2/24
```

4. **CONFIGURACIÓN FR DEL ROUTER LIMA**:

- Se comprueba que la interfaz serial 0/0 estará desactivada a raíz del encapsulamiento HDLC que mantiene.

```
LIMA#sh protocols
Global values:
 Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
Serial0/0 is up, line protocol is down
Serial0/1 is down, line protocol is down
```

- Encapsulamiento Frame Relay.

a. Al habilitar el encapsulamiento se muestra un mensaje indicando que la interfaz serial 0/0 está activa.

b. Se comprueba el estado de la interfaz.

```
LIMA#
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#int s0/0
LIMA(config-if)#encapsulation frame-relay
LIMA(config-if)#ip add 192.168.10.1 255.255.255.0
LIMA(config-if)#no shut
LIMA(config-if)#^Z
LIMA#sh protocols
Global values:
  Internet Protocol routing is enabled
 FastEthernet0/0 is administratively down, line protocol is down
 Serial0/0 is up, line protocol is up
   Internet address is 192.168.10.1/24
 Serial0/1 is down, line protocol is down
```

5. **COMPLETANDO LA CONFIGURACIÓN DE INTERFACES**:

```
AREQUIPA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AREQUIPA(config)#int f0/0
AREQUIPA(config-if)#no shut
AREQUIPA(config-if)#no kee
AREQUIPA(config-if)#ip add 192.168.22.1 255.255.255.0
*Mar  1 00:34:37.320: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:34:38.322: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

```
LIMA(config-if)#
LIMA(config-if)#int f0/0
LIMA(config-if)#no shut
LIMA(config-if)#no kee
LIMA(config-if)#ip add 192.168.11.1 255.255.255.0
*Mar  1 00:36:37.320: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:36:38.322: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

CASO II: ENRUTAMIENTO EIGRP (AS 64500)

Considerando que tiene una conexión hacia Internet, deberá habilitarse una ruta por defecto y redistribuirse dentro del AS 64500. Asimismo, el router Lima presenta cuatro redes, las cuales se deberán publicar mediante EIGRP y posteriormente realizar un resumen manual para su publicación.

1. **ENRUTAMIENTO EIGRP**

```
AREQUIPA(config)#router eigrp 64500
AREQUIPA(config-router)#no aut
AREQUIPA(config-router)#net 192.168.22.0
AREQUIPA(config-router)#net 192.168.10.0
```

```
LIMA(config)#router eigrp 64500
LIMA(config-router)#no auto
LIMA(config-router)#net 192.168.10.0
LIMA(config-router)#net 192.168.10.0
```

2. **VERIFICANDO**

- Se revisa la tabla de enrutamiento en el router Arequipa para comprobar la publicación de redes.

```
AREQUIPA#sh ip rou
……< resultado omitido >……..
Gateway of last resort is not set
C    192.168.10.0/24 is directly connected, Serial0/1
C    192.168.22.0/24 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/20514560] via 192.168.10.1, 00:01:50, Serial0/1
```

- Se realiza una prueba de conectividad y completamos la prueba.

```
AREQUIPA#ping 192.168.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
```

- Se revisa la tabla de enrutamiento en router Lima para comprobar la publicación de redes.

```
LIMA#sh ip rou
……< resultado omitido >……..
Gateway of last resort is not set
C    192.168.10.0/24 is directly connected, Serial0/0
C    192.168.11.0/24 is directly connected, FastEthernet0/0
D    192.168.22.0/24 [90/20514560] via 192.168.10.2, 00:00:16, Serial0/0
```

- Se realiza una prueba de conectividad y completamos la prueba.

```
LIMA#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
```

3. **REDES ADICIONALES**

- Agregamos interfaces loopback para representar otras redes conectadas al router Lima.

```
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#int l0
LIMA(config-if)#ip add 172.16.1.1 255.255.255.255
LIMA(config-if)#exit
LIMA(config)#int l1
LIMA(config-if)#ip add 172.16.2.1 255.255.255.255
LIMA(config-if)#exit
LIMA(config-if)#int l2
```

```
LIMA(config-if)#ip add 172.16.3.1 255.255.255.255
LIMA(config-if)#exit
iLIMA(config-if)#int l3
LIMA(config-if)#ip add 172.16.0.1 255.255.255.255
LIMA(config-if)#exit
LIMA(config)#router eigrp 64530
LIMA(config-router)#net 172.16.0.0 0.0.0.255
LIMA(config-router)#net 172.16.0.0 0.0.0.255
LIMA(config-router)#net 172.16.1.0 0.0.0.255
LIMA(config-router)#net 172.16.2.0 0.0.0.255
LIMA(config-router)#^Z
LIMA#wr
Building configuration...
```

- Se revisa la tabla de enrutamiento en el router Arequipa para comprobar la publicación de redes.

```
AREQUIPA#sh ip rou
……< resultado omitido >…….
Gateway of last resort is not set
C   192.168.10.0/24 is directly connected, Serial0/1
    172.16.0.0/32 is subnetted, 4 subnets
D      172.16.1.1 [90/20640000] via 192.168.10.1, 00:00:21, Serial0/1
D      172.16.0.1 [90/20640000] via 192.168.10.1, 00:00:25, Serial0/1
D      172.16.3.1 [90/20640000] via 192.168.10.1, 00:00:12, Serial0/1
D      172.16.2.1 [90/20640000] via 192.168.10.1, 00:00:15, Serial0/1
D   192.168.11.0/24 [90/20514560] via 192.168.10.1, 00:02:59, Serial0/1
C   192.168.22.0/24 is directly connected, FastEthernet0/0
```

4. SUMARIZACIÓN MANUAL

- Se realiza la sumarización de las redes definidas mediante las interfaces loopback, lo cual permitirá una tabla de enrutamiento más pequeña.

```
LIMA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#int s0/0
LIMA(config-if)#ip summary-address eigrp 64500 172.16.0.0 255.255.248.0
LIMA(config-if)#^Z
```

5. CONFIGURANDO REDISTRIBUCIÓN DE RUTA POR DEFECTO

- El router Arequipa presenta una conexión hacia un proveedor de servicios por lo que se habilita una ruta por defecto, la cual se deberá redistribuir mediante EIGRP en el sistema autónomo.

```
AREQUIPA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AREQUIPA(config)#int l0
AREQUIPA(config-if)#ip add 172.17.3.22 255.255.255 2.0
AREQUIPA(config-if)#exit
AREQUIPA(config)#ip route 0.0.0.0 0.0.0.0 l0
AREQUIPA(config)#router eigrp 64500
AREQUIPA(config-router)#redistribute static
AREQUIPA(config-router)#^Z
AREQUIPA#wr
Building configuration...
*Mar  1 01:14:12.097: %SYS-5-CONFIG_I: Configured from console by console
```

6. TABLA FINAL DE ENRUTAMIENTO

- ROUTER LIMA:

```
LIMA#sh ip rou
……< resultado omitido >……..
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.1/32 is directly connected, Loopback0
D       172.16.0.0/22 is a summary, 00:03:31, Null0
C       172.16.0.1/32 is directly connected, Loopback3
C       172.16.3.1/32 is directly connected, Loopback2
C       172.16.2.1/32 is directly connected, Loopback1
C    192.168.11.0/24 is directly connected, FastEthernet0/0
D    192.168.22.0/24 [90/20514560] via 192.168.10.2, 00:02:59, Serial0/0
D*EX 0.0.0.0/0 [170/20640000] via 192.168.10.2, 00:00:19, Serial0/0
LIMA#
```

- ROUTER AREQUIPA:

```
AREQUIPA#sh ip route
……< resultado omitido >……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/1
     172.17.0.0/22 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Loopback0
     172.16.0.0/22 is subnetted, 1 subnets
D       172.16.0.0 [90/20640000] via 192.168.10.1, 00:04:55, Serial0/1
D    192.168.11.0/24 [90/20514560] via 192.168.10.1, 00:04:55, Serial0/1
C    192.168.22.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Loopback0
```

7. Información en el switch Frame Relay

- Configuración activa del router Cisco que trabaja como switch Frame Relay.

```
SW-FR#show runn
!
frame-relay switching
!
!
!
!
!
!
!
 interface FastEthernet0/0
 no ip address
 shutdown
 speed auto
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
  frame-relay lmi-type ansi
 frame-relay intf-type dce
```

```
 frame-relay route 112 interface Serial0/1 211
!
interface Serial0/1
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 211 interface Serial0/0 112
!
!
```

- Se observa la información del PVC creado para esta conexión, donde se mencionan los DLCI y las estadísticas respecto del tráfico de paquetes.

```
SW-FR#sh frame-relay pvc
PVC Statistics for interface Serial0/0 (Frame Relay DCE)
          Active    Inactive     Deleted      Static
 Local       0          0          0          0
 Switched     1          0          0          0
 Unused       0          0          0          0
DLCI = 112, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0
 input pkts 60          output pkts 52          in bytes 4138
 out bytes 3626          dropped pkts 2          in pkts dropped 2
 out pkts dropped 0              out bytes dropped 0
 in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
 out BECN pkts 0          in DE pkts 0          out DE pkts 0
 out bcast pkts 0        out bcast bytes 0
 30 second input rate 0 bits/sec, 0 packets/sec
 30 second output rate 0 bits/sec, 0 packets/sec
 switched pkts 59
 Detailed packet drop counters:
 no out intf 0          out intf down 0          no out PVC 0
 in PVC down 0          out PVC down 2          pkt too big 0
 shaping Q full 0        pkt above DE 0          policing drop 0
  pvc create time 00:59:17, last time pvc status changed 00:18:50

PVC Statistics for interface Serial0/1 (Frame Relay DCE)
          Active    Inactive     Deleted      Static
 Local       0          0          0          0
 Switched     1          0          0          0
 Unused       0          0          0          0
DLCI = 211, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/1
 input pkts 53          output pkts 59          in bytes 3660
 out bytes 4104          dropped pkts 2          in pkts dropped 2
 out pkts dropped 0              out bytes dropped 0
 in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
 out BECN pkts 0          in DE pkts 0          out DE pkts 0
 out bcast pkts 0        out bcast bytes 0
 30 second input rate 0 bits/sec, 0 packets/sec
 30 second output rate 0 bits/sec, 0 packets/sec
 switched pkts 52
 Detailed packet drop counters:
 no out intf 0          out intf down 0          no out PVC 0
 in PVC down 0          out PVC down 2          pkt too big 0
 shaping Q full 0        pkt above DE 0          policing drop 0
  pvc create time 00:58:02, last time pvc status changed 00:18:17
```

8. Deshabilitar el enrutamiento EIGRP para permitir la configuración del siguiente protocolo (OSPF)

CASO III: ENRUTAMIENTO OSPF (ÁREA 0)

En el modo NBMA (redes sin difusión), el DR y BDR necesitan tener una conectividad física total con todos los routers que estén conectados a la nube. Además, necesitan tener una lista estática de todos los demás routers debido a la falta de posibilidades de difusión (una lista de todos los vecinos, con el uso del comando **neighbor**).

1. **CONFIGURACIÓN DE ENRUTAMIENTO**:

   - Como se observa, la configuración de enrutamiento es la misma, con el agregado del comando neighbor, seguido del IP del router con el que se quiere establecer vecindad.

```
LIMA#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#no router eigrp 64500
LIMA(config)#ROUTER OSPF 1
LIMA(config-router)#NET 192.168.10.0 0.0.0.255 AREA 0
LIMA(config-router)#NET 192.168.11.0 0.0.0.255 AREA 0
LIMA(config-router)#neighbor 192.168.10.2
LIMA(config-router)#net 172.16.0.0 0.0.0.255 area
LIMA(config-router)#net 172.16.1.0 0.0.0.255 area
LIMA(config-router)#net 172.16.2.0 0.0.0.255 area
```

   - Con el comando ***default-Information Originate*** se redistribuye la ruta por defecto.

```
AREQUIPA#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
AREQUIPA(config)# no router eigrp 64500
AREQUIPA(config)# ROUTER OSPF 1
AREQUIPA(config-router)#NET 192.168.10.0 0.0.0.0.255 AREA 0
AREQUIPA(config-router)#NET 192.168.22.0 0.0.0.255 AREA 0 .
AREQUIPA(config-router)#neighbor 192.168.10.1
AREQUIPA(config-router)#default-Information Originate
```

***Nota**: El comando **neighbor**, por las posibilidades de usar otros modos con redes sin difusión, puede no emplearse para esas configuraciones. Asimismo, se puede añadir de forma opcional la configuración de prioridad, intervalo de sondeo o el costo.*

2. **TABLA DE ENRUTAMIENTO**:

   - Se revisa la tabla de enrutamiento en ambos routers para comprobar la publicación de redes mediante OSPF (se resaltan las redes publicadas).
   - Ambos routers reciben la información de enrutamiento.

```
LIMA#sh ip route
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
C       172.16.3.0 is directly connected, Loopback3
C    192.168.11.0/24 is directly connected, FastEthernet0/0
O    192.168.22.0/24 [110/782] via 192.168.10.2, 00:01:30, Serial0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.10.2, 00:01:30, Serial0/0
```

```
AREQUIPA#sh ip route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C   192.168.10.0/24 is directly connected, Serial0/1
    172.17.0.0/22 is subnetted, 1 subnets
C      172.17.0.0 is directly connected, Loopback0
    172.16.0.0/32 is subnetted, 4 subnets
O      172.16.1.1 [110/782] via 192.168.10.1, 00:02:01, Serial0/1
O      172.16.0.1 [110/782] via 192.168.10.1, 00:02:01, Serial0/1
O      172.16.3.1 [110/782] via 192.168.10.1, 00:02:01, Serial0/1
O      172.16.2.1 [110/782] via 192.168.10.1, 00:02:01, Serial0/1
O   192.168.11.0/24 [110/782] via 192.168.10.1, 00:02:02, Serial0/1
C   192.168.22.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Loopback0
```

3. TABLA DE VECINOS

- Verificamos la elección del DR y BDR, con la indicación del ID para cada router.

```
AREQUIPA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        1   FULL/BDR        00:01:30    192.168.10.1    Serial0/1
```

```
LIMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.17.3.22       1   FULL/DR         00:01:35    192.168.10.2    Serial0/0
```

4. VERIFICANDO

- Se realiza una prueba de conectividad.

```
AREQUIPA#ping 192.168.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
```

```
LIMA#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
```

5. CONFIGURACIÓN FINAL

```
AREQUIPA#SH
!
!
interface Loopback0
 ip address 172.17.3.22 255.255.252.0
!
interface FastEthernet0/0
 ip address 192.168.22.1 255.255.255.0
 no keepalive
 speed auto
```

```
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1
 ip address 192.168.10.2 255.255.255.0
 encapsulation frame-relay
 !
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.22.0 0.0.0.255 area 0
 neighbor 192.168.10.1
 default-information originate
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 Loopback0
 no ip http server
 !
 !
```

```
LIMA# sh runn
!
!
interface Loopback0
 ip address 172.16.0.1 255.255.255.0
!
interface Loopback1
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback2
 ip address 172.16.2.1 255.255.255.0
!
interface Loopback3
 ip address 172.16.3.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.11.1 255.255.255.0
 speed auto
 no keepalive
!
interface Serial0/0
 ip address 192.168.10.1 255.255.255.0
 encapsulation frame-relay
!
interface Serial0/1
 no ip address
 !
router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 neighbor 192.168.10.2
!
```

CASO IV: ENRUTAMIENTO RIP v2

No es común emplear el protocolo RIP en enlaces Frame Relay, pero si éste fuera el caso, no hay necesidad de una configuración adicional, como se muestra. En otras situaciones deberá deshabilitarse el horizonte dividido.

1. **CONFIGURACION DE ENRUTAMIENTO:**
   - Se habilita la ruta por defecto, como en los casos anteriores, y se redistribuye.

```
AREQUIPA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AREQUIPA(config)# ip route 0.0.0.0 0.0.0.0 Loopback0
AREQUIPA(config)#router rip
AREQUIPA(config-router)#ver 2
AREQUIPA(config-router)#no auto-summary
AREQUIPA(config-router)#net 192.168.10.0
AREQUIPA(config-router)#net 192.168.10.00.0 .0 2.02.0
AREQUIPA(config-router)#redistribute static
AREQUIPA(config-router)#
```

```
LIMA(config)#router rip
LIMA(config-router)#ver 2
LIMA(config-router)#no auto-summary
LIMA(config-router)#net 192.168.10.0
LIMA(config-router)#net 192.168.11.0
LIMA(config-router)#net 172.16.0.0
LIMA(config-router)#^Z
```

2. **TABLA DE ENRUTAMIENTO:**
   - Se revisa la tabla de enrutamiento en ambos routers para comprobar la publicación de redes mediante RIP v2 (se resaltan las redes publicadas).
   - Se comprueba que ambos routers reciban la información de enrutamiento RIP.

```
LIMA#sh ip route
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
C       172.16.3.0 is directly connected, Loopback3
C    192.168.11.0/24 is directly connected, FastEthernet0/0
R    192.168.22.0/24 [120/1] via 192.168.10.2, 00:00:06, Serial0/0
R*   0.0.0.0/0 [120/1] via 192.168.10.2, 00:00:06, Serial0/0
```

```
AREQUIPA#sh ip rou
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/1
     172.17.0.0/22 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Loopback0
     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.0.0 [120/1] via 192.168.10.1, 00:00:23, Serial0/1
R       172.16.1.0 [120/1] via 192.168.10.1, 00:00:23, Serial0/1
R       172.16.2.0 [120/1] via 192.168.10.1, 00:00:23, Serial0/1
R       172.16.3.0 [120/1] via 192.168.10.1, 00:00:23, Serial0/1
R    192.168.11.0/24 [120/1] via 192.168.10.1, 00:00:24, Serial0/1
C    192.168.22.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Loopback0
```

3. Para reducir el tamaño de la tabla de enrutamiento, sumarizamos las redes en el router Lima.

```
LIMA(config)#int s0/0
LIMA(config-if)#ip summary-address rip 172.16..0  0.0 2552 .255.252.0
LIMA(config-if)#^Z
LIMA#wr
Building configuration...
[OK]
```

4. La tabla de enrutamiento en el router Lima no cambia, sólo es necesario verificarlo en el router Arequipa, aunque debe considerarse el período de espera (hold on time).

```
LIMA#sh ip rout
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
C       172.16.3.0 is directly connected, Loopback3
C    192.168.11.0/24 is directly connected, FastEthernet0/0
R    192.168.22.0/24 [120/1] via 192.168.10.2, 00:00:03, Serial0/0
R*   0.0.0.0/0 [120/1] via 192.168.10.2, 00:00:03, Serial0/0
```

```
AREQUIPA#sh ip route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C    192.168.10.0/24 is directly connected, Serial0/1
     172.17.0.0/22 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Loopback0
     172.16.0.0/22 is subnetted, 1 subnets
R       172.16.0.0 [120/1] via 192.168.10.1, 00:00:11, Serial0/1
R    192.168.11.0/24 [120/1] via 192.168.10.1, 00:00:11, Serial0/1
C    192.168.22.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Loopback0
```

5. Finalmente la base de datos de RIP muestra en detalle la información que recibe cada router.

```
LIMA#sh ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 192.168.10.2, 00:00:08, Serial0/0
172.16.0.0/16    auto-summary
172.16.0.0/22    int-summary
172.16.0.0/24    directly connected, Loopback0
172.16.1.0/24    directly connected, Loopback1
172.16.2.0/24    directly connected, Loopback2
172.16.3.0/24    directly connected, Loopback3
192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, Serial0/0
192.168.11.0/24    auto-summary
192.168.11.0/24    directly connected, FastEthernet0/0
192.168.22.0/24    auto-summary
192.168.22.0/24
    [1] via 192.168.10.2, 00:00:09, Serial0/0
```

```
AREQUIPA#sh ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0    redistributed
    [1] via 0.0.0.0,
172.16.0.0/16    auto-summary
172.16.0.0/22
    [1] via 192.168.10.1, 00:00:24, Serial0/1
192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, Serial0/1
192.168.11.0/24    auto-summary
192.168.11.0/24
    [1] via 192.168.10.1, 00:00:24, Serial0/1
192.168.22.0/24    auto-summary
192.168.22.0/24    directly connected, FastEthernet0/0
AREQUIPA#
```

6. Configuración final de cada router.

```
LIMA#sh runn
!
!
Loopback0
 ip address 172.16.0.1 255.255.255.0
!
interface Loopback1
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback2
 ip address 172.16.2.1 255.255.255.0
!
interface Loopback3
 ip address 172.16.3.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.11.1 255.255.255.0
 speed auto
 no keepalive
!
interface Serial0/0
 ip address 192.168.10.1 255.255.255.0
 encapsulation frame-relay
ip summary-address rip 172.16..0  0.0 2552 .255.252.0
!
interface Serial0/1
 no ip address
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.10.0
 network 192.168.11.0
 no auto-summary
!
!
```

CONCLUSIONES

_____

Laboratorio N° 6 - Topologías Multipunto

INTRODUCCIÓN

La característica fundamental de esta topología es que existe un origen y múltiples destinos. Las líneas multipunto son utilizadas para reducir el número de líneas requeridas para conectar estaciones y reducir el costo de éstas. El diseño de una red de este tipo es generalmente más complejo que en una red de punto a punto.

Además, se implementan algunos conceptos de control de acceso a una línea de multipunto, para evitar conflictos por el uso del canal, ya que es el único medio pasivo de comunicación y están interconectadas todas las estaciones de trabajo. Una red de este tipo es generalmente más compleja.

Las redes NBMA son aquellas que soportan más de dos routers pero que no tienen capacidad de difusión. Frame Relay, ATM, X.25 son algunos ejemplos de redes NBMA. La selección del DR se convierte en un tema importante ya que el DR y el BDR deben tener conectividad física total con todos los routers de la red.

OBJETIVOS

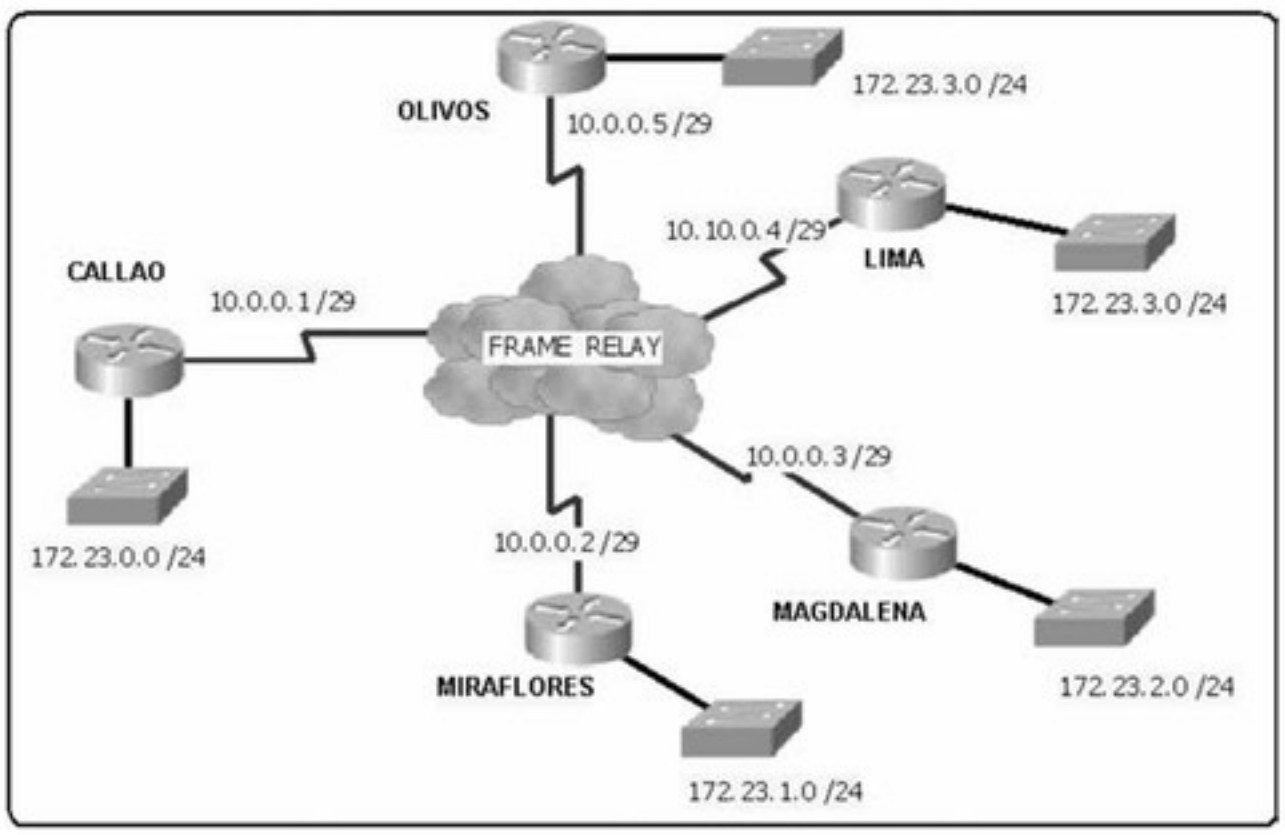
- Implementación del protocolo de OSPF en una red multipunto sobre la topología Frame Relay.
- Implementación del protocolo de OSPF en una red punto – multipunto sobre la topología Frame Relay.

DESCRIPCIÓN

Se plantean dos casos para configurar el protocolo OSPF: el primero es una implementación de la red multipunto y el segundo caso se trata de una red punto –multipunto. Para ambos casos considere el uso de un router como switch Frame Relay que simule dicha conexión o, en su reemplazo, el Adtran Atlas 550.

CASO 1:

La topología estará implementada mediante un PVC por cada sucursal y cuatro PVC desde el router Callao, con topología punto-multipunto, logrando que todos los PVC estén en la misma subred 10.0.0.0 /29, enrutados por OSPF en área 0, por lo cual se elegirá un DR y BDR para el vecindario.



DESARROLLO:

1. Realice las rutinas de diagnóstico y deje listos los equipos para su configuración.
2. Realice la conexión física de los equipos en base a la topología de red.
3. Habilite la opción de captura de texto en el emulador (Hyperterminal).
4. Realice la configuración básica y avanzada mediante el enrutamiento OSPF, como se describe en el resumen de configuración.
5. **Elección de un DR y un BDR**
   - Los routers de un entorno multiacceso deben elegir un Router Designado (DR) y un Router Designado de Reserva (BDR) para que representen a la red. Un DR lleva a cabo tareas de envío y sincronización. El BDR sólo actuará si el DR falla. Cada router debe establecer una adyacencia con el DR y el BDR.
   - El comando **ip ospf priority** sirve para elegir siempre como DR al router Callao, ya que no hay interfaces loopback configuradas.
6. **Configuración final de cada routera**
   a. El router Callao centraliza las conexiones, por lo que la subinterfaz es multipunto; asimismo, debe contar con un mapa hacia cada vecino a comunicarse mediante su DLCI.
   b. Son importantes los comandos complementarios para mantener la difusión de los LSU dentro de OSPF (ip ospf network broadcast).

```
CALLAO#sh runn
!
!
interface FastEthernet0/0
 ip address 172.23.0.1 255.255.255.0
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 ip ospf network broadcast
!
interface Serial0/0.100 multipoint
 ip address 10.0.0.1 255.255.255.248
 frame-relay map ip 10.0.0.2 666 broadcast
 frame-relay map ip 10.0.0.3 777 broadcast
 frame-relay map ip 10.0.0.4 888 broadcast
 frame-relay map ip 10.0.0.5 999 broadcast
 ip ospf network broadcast
 ip ospf priority 2
!
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 172.23.0.0 0.0.0.255 area 0
!
end
```

- Los routers Miraflores y Magdalena presentan una configuración parecida al router Callao, con la diferencia de que se trabaja con las interfaces directamente:

```
Miraflores#sh runn
!
!
interface FastEthernet0/0
 ip address 172.23.1.1 255.255.255.0
!
interface Serial0/0
 ip address 10.0.0.2 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 100 broadcast
 frame-relay map ip 10.0.0.3 100 broadcast
 frame-relay map ip 10.0.0.4 100 broadcast
 frame-relay map ip 10.0.0.5 100 broadcast
 frame-relay interface-dlci 100
 ip ospf network broadcast
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 172.23.1.0 0.0.0.255 area 0
!
end
```

```
Magdalena#sh runn
!
!
interface FastEthernet0/0
 ip address 172.23.2.1 255.255.255.0
!
interface Serial0/0
 ip address 10.0.0.3 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 200 broadcast
 frame-relay map ip 10.0.0.2 200 broadcast
 frame-relay map ip 10.0.0.4 200 broadcast
 frame-relay map ip 10.0.0.5 200 broadcast
 frame-relay interface-dlci 200
 ip ospf network broadcast
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 172.23.2.0 0.0.0.255 area 0
!
end
```

- **Los routers Lima y Olivos presentan l**a misma configuración que los routers Miraflores y Magdalena, cambiando únicamente lo que respecta a las subredes conectadas y no realizando el mapeo Frame Relay en su propia IP de la interfaz WAN.

7. **Verificación de enrutamiento:**

Para el caso sólo es necesario verificar en el router Callao, ya que concentra todas las conexiones.

- Tabla de vecinos OSPF:

```
CALLAO#sh ip ospf nei
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.23.4.1        1   FULL/BDR        00:00:09    10.0.0.5        Serial0/0.100
172.23.3.1        1   FULL/DROTHER    00:00:09    10.0.0.4        Serial0/0.100
172.23.1.1        1   FULL/DROTHER    00:00:09    10.0.0.2        Serial0/0.100
172.23.2.1        1   FULL/DROTHER    00:00:09    10.0.0.3        Serial0/0.100
```

- Tabla de enrutamiento:

```
CALLAO#sh ip route
……….< resultado omitido >……..
Gateway of last resort is not set
     10.0.0.0/29 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial0/0.100
     172.23.0.0/24 is subnetted, 5 subnets
C       172.23.0.0 is directly connected, FastEthernet0/0
O       172.23.1.0 [110/65] via 10.0.0.2, 00:12:15, Serial0/0.100
O       172.23.2.0 [110/65] via 10.0.0.3, 00:12:15, Serial0/0.100
O       172.23.3.0 [110/65] via 10.0.0.4, 00:12:15, Serial0/0.100
O       172.23.4.0 [110/65] via 10.0.0.5, 00:09:20, Serial0/0.100
CALLAO#
```

- Mapa de enlaces Frame Relay.

```
CALLAO#sh frame-relay  map
Serial0/0.100 (up): ip 10.0.0.2 dlci 666, static, broadcast, CISCO, status defined, active
Serial0/0.100 (up): ip 10.0.0.3 dlci 777, static, broadcast, CISCO, status defined, active
Serial0/0.100 (up): ip 10.0.0.4 dlci 888, static, broadcast, CISCO, status defined, active
Serial0/0.100 (up): ip 10.0.0.5 dlci 999, static, broadcast, CISCO, status defined, active
CALLAO#
```

- Verificamos, a su vez, el router Miraflores y comprobamos las redes publicadas mediante OSPF.

```
Miraflores#sh ip route
……….< resultado omitido >……..
Gateway of last resort is not set
     10.0.0.0/29 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial0/0
     172.23.0.0/24 is subnetted, 5 subnets
O       172.23.0.0 [110/65] via 10.0.0.1, 00:27:21, Serial0/0
C       172.23.1.0 is directly connected, FastEthernet0/0
O       172.23.2.0 [110/65] via 10.0.0.3, 00:27:21, Serial0/0
O       172.23.3.0 [110/65] via 10.0.0.4, 00:27:21, Serial0/0
O       172.23.4.0 [110/65] via 10.0.0.5, 00:24:42, Serial0/0
Miraflores#
```

8. **Diagnóstico de conectividad:**

- Desde un Host de la red Lan del router Olivos hacia un Host de la red Lan del router Miraflores:

```
C:\Users\hector>ping 172.23.1.2

Haciendo ping a 172.23.1.2 con 32 bytes de datos:

Respuesta desde 172.23.1.2: bytes=32 tiempo=182ms TTL=125
Respuesta desde 172.23.1.2: bytes=32 tiempo=167ms TTL=125
Respuesta desde 172.23.1.2: bytes=32 tiempo=132ms TTL=125
Respuesta desde 172.23.1.2: bytes=32 tiempo=166ms TTL=125

Estadísticas de ping para 172.23.1.2:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 132ms, Máximo = 182ms, Media = 162ms
```

***Nota**: De no encontrarse el mapeo Frame Relay a una IP que es puerta de enlace a una red o subred, el router no podrá encapsular el paquete con el DLCI destino, ya que esta topología es multiacceso, por lo cual se "asemeja" al funcionamiento de Ethernet.*

OSPF realiza la convergencia, muestra el destino en la tabla de enrutamiento, pero esta información no asegura que el paquete llegue a destino, ya que en este caso se encapsula en una trama de CAPA 2 y no posee el DLCI destino.

- La convergencia se da porque en esta topología la base de datos OSPF llega desde el DR (Callao) y no desde cada router.
- En el router Olivos, por su configuración, sólo se indicará que el router Olivos es su único vecino.

```
OLIVOS#sh ip ospf neibor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.23.0.1        2   FULL/DR         00:00:28    10.0.0.1        Serial0/0
```

- Verificamos el protocolo habilitado.

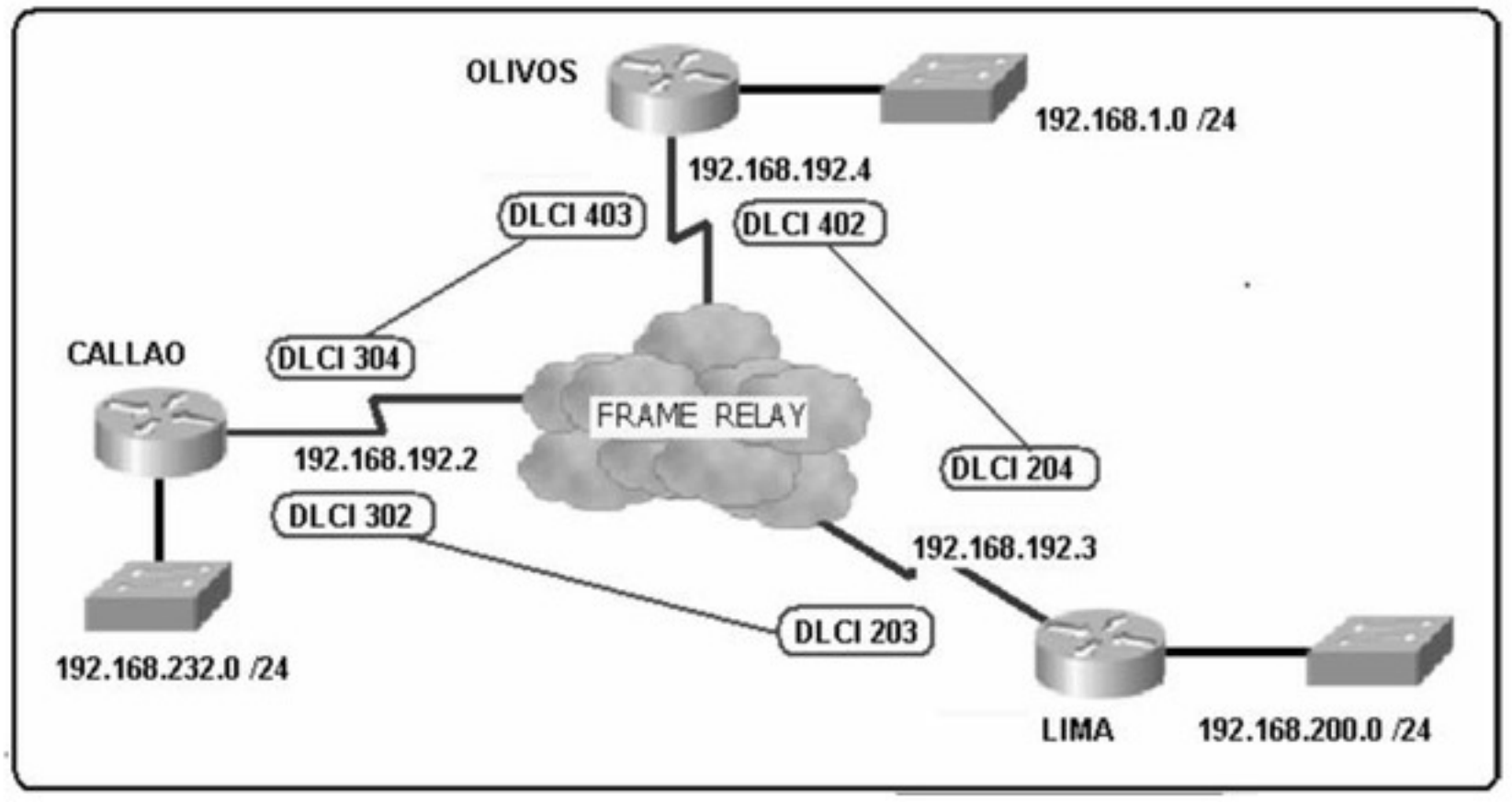
```
OLIVOS#sh ip protocol
Routing Protocol is "ospf 1"
  ....
  Router ID 172.23.4.1
  Routing for Networks:
    10.0.0.0 0.0.0.7 area 0
    172.23.4.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.1             110      00:09:24
```

CONCLUSIONES Y/U OBSERVACIONES

_____

_____

CASO 2: CONFIGURACIÓN OSPF PUNTO A MULTIPUNTO SOBRE FRAME RELAY



DESARROLLO:

1. CONFIGURACIÓN DE ROUTER:
   - Implementar la red de acuerdo al diagrama, configurando las interfaces FastEthernet como se muestra:

```
LIMA#configure terminal
LIMA(config)#Interfase fastEthernet 0/0
LIMA(config-if)#no shutdown
LIMA(config-if)#ip add 192.168.200.2 255.255.255.0
```

```
CALLAO#configure terminal
CALLAO(config)#Interfase fastEthernet 0/0
CALLAO(config-if)#no shutdown
CALLAO(config-if)#ip add 192.168.232.3 255.255.255.0
```

```
OLIVOS #configure terminal
OLIVOS (config)#Interfase fastEthernet 0/0
OLIVOS (config-if)#no shutdown
OLIVOS (config-if)#ip add 192.168.1.4 255.255.255.0
```

2. Note que esta configuración incluye los comandos **frame-relay map** que son típicamente usados con sub-interfaces Frame Relay. Estos comandos son necesarios aquí para que se pueda configurar el tráfico de broadcast (digitando el comando broadcast). Sin esta configuración, el tráfico multicast de OSPF no se reenviará correctamente sobre la topología Frame Relay.

```
LIMA#configure terminal
LIMA(config)#Interfase serial 0/0
LIMA(config-if)#no shutdown
LIMA(config-if)#ip add 192.168.192.2 255.255.255.0
LIMA(config-if)#encapsulation frame-relay
LIMA(config-if)#frame-relay map ip 192.168.192.3 203 broadcast
LIMA(config-if)#frame-relay map ip 192.168.192.4 204 broadcast
LIMA(config-if)#ip ospf network point-to-multipoint
```

```
CALLAO#configure terminal
CALLAO(config)#Interfase serial 0/0
CALLAO(config-if)#no shutdown
CALLAO(config-if)#ip add 192.168.192.3 255.255.255.0
CALLAO(config-if)#encapsulation frame-relay
CALLAO(config-if)#frame-relay map ip 192.168.192.2 302 broadcast
CALLAO(config-if)#frame-relay map ip 192.168.192.4 304 broadcast
CALLAO(config-if)#ip ospf network point-to-multipoint
```

```
OLIVOS#configure terminal
OLIVOS(config)#Interfase serial 0/0
OLIVOS(config-if)#no shutdown
OLIVOS (config-if)#ip add 192.168.192.4 255.255.255.0
OLIVOS (config-if)#encapsulation frame-relay
OLIVOS (config-if)#frame-relay map ip 192.168.192.2 402 broadcast
OLIVOS (config-if)#frame-relay map ip 192.168.192.3 403 broadcast
OLIVOS (config-if)#ip ospf network point-to-multipoint
```

3. Use los comandos **show frame-relay pvc** y **show frame-relay map** para verificar problemas de conectividad. Reinicie el switch Frame Relay para solucionar posibles problemas de conectividad.

   Preste atención al estado de PVC:

   - Si el PVC indica STATUS=DELETED, aquí no está definido su PVC en el switch Frame Relay.
   - Si el PVC indica STATUS=INACTIVE, este es un problema de conexión.

```
OLIVOS#show frame-relay pvc
PVC Statistics for interface Serial0/0 (Frame Relay DTE)
        Active Inactive Deleted Static
Local     2      0      0      0
Switched  0      0      0      0
Unused    0      0      0      0

DLCI = 402, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0
input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:02:04, last time pvc status changed 00:01:09

DLCI = 403, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0
input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:01:17, last time pvc status changed 00:01:12
```

- Verifique la operación con un ping hacia cada router.

```
OLIVOS#ping 192.168.192.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.192.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/22 ms
```

```
LIMA#show frame-relay map
Serial0/0 (up): ip 192.168.192.2 dlci 402(0x12,0x420), static,broadcast,
CISCO, status defined, active
Serial0/0 (up): ip 192.168.192.3 dlci 403(0x11,0x410), static,broadcast,
CISCO, status defined, active
```

4. CONFIGURE EL ENRUTAMIENTO OSPF
   - Ejecute OSPF sobre la red point-to-multipoint.
   - Emplee los siguientes comandos:

```
LIMA(config)#router ospf 1
LIMA(config-router)#network 192.168.200.0 0.0.0.255 area 0
LIMA(config-router)#network 192.168.192.0 0.0.0.255 area 0
```

```
CALLAO(config)#router ospf 1
CALLAO(config-router)#network 192.168.232.0 0.0.0.255 area 0
CALLAO(config-router)#network 192.168.192.0 0.0.0.255 area 0
```

```
OLIVOS(config)#router ospf 1
OLIVOS(config-router)#network 192.168.1.0 0.0.0.255 area 0
OLIVOS(config-router)#network 192.168.192.0 0.0.0.255 area 0
```

5. Verifique la publicación de redes:

```
LIMA#sh ip route
Gateway of last resort is not set
192.168.192.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.192.0/24 is directly connected, Serial0/0
O 192.168.192.3/32 [110/64] via 192.168.192.1, 00:04:43,Serial0/0
O 192.168.192.4/32 [110/64] via 192.168.192.1, 00:04:43,Serial0/0
C 192.168.200.0/24 is directly connected, FastEthernet0/0
O 192.168.232.0/24 [110/129] via 192.168.192.1, 00:04:43,Serial0/0
O 192.168.1.0/24 [110/65] via 192.168.192.1, 00:05:45,Serial0/0
```

- Si cada router tiene completa su tabla, se incluyen rutas hacia las redes 192.168.10.0 /24, 192.168.200.0 /24 y 192.168.232.0 /24; se configuró correctamente OSPF para operar sobre Frame Relay.

```
LIMA#ping 192.168.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 59/60/64 ms
R2#ping 192.168.192.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.192.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 59/60/60 ms
```

6. Finalmente verifique la tabla de vecinos.

```
LIMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.192.4     1   FULL/-          00:01:30    192.168.192.4   Serial0/0
192.168.232.3     1   FULL/-          00:01:18    192.168.192.3   Serial0/0
```

CONCLUSIONES Y/U OBSERVACIONES

CASOS DE ESTUDIO

Integra los diversos temas que se presentan en los capítulos anteriores, sumándose la configuración de temas como el servicio DHCP local y remoto, seguridad mediante las listas de control de acceso, autenticación local para el acceso por terminal virtual y configuración del servidor TACACS+; tanto para ambientes inalámbricos como para redes LAN y WAN.

LABORATORIO N° 1: RIP

El laboratorio repite un esquema anterior implementado con PPP y RIPv2. Para este caso, se ha complementado con el servicio DHCP donde se aplica el comando helper address. Así mismo, se da la traducción de direcciones por puerto (PAT) en uno de los enlaces.

LABORATORIO N° 2: VLAN CON ENRUTAMIENTO DINÁMICO DE DOS PROTOCOLOS POR CONEXIÓN FRAME RELAY

Se ha desarrollado una implementación de red en Frame Relay, en dos partes. En la primera parte se configura el enlace WAN mediante los protocolos de enrutamiento EIGRP y RIP, y su redistribución de rutas; considerar el uso de un switch capa 3. Para la red LAN se habilitan VLAN, intervlan y el servicio DHCP. La segunda parte modifica el enrutamiento RIP por enrutamiento estático hacia un ISP, por lo que se habilita el servicio PAT.

LABORATORIO N° 3:

El laboratorio integra cuatro casos prácticos desarrollados sobre una topología base con conexión a Internet y hacia una nueva sucursal, los cuales se describen a continuación:

CASO 1: Enrutamiento estático y por defecto con encapsulamiento HDLC.

CASO 2: Agregar la configuración de red VLAN y conexión inalámbrica.

CASO 3: Implementación de la traducción de direcciones por sobrecarga (PAT).

CASO 4: Modificación del enlace hacia la sucursal con Frame Relay, con enrutamiento EIGRP.

LABORATORIO N° 4: REDISTRIBUCION OSPF Y EIGRP

Se plantea la configuración de una topología con enrutamiento de ruta por defecto hacia Internet; OSPF, para una red multiacceso, y EIGRP para conexiones punto a punto, las cuales se redistribuyen y permiten la conectividad desde cualquier punto. Así mismo, se configura la traducción de direcciones.

LABORATORIO N°5: SWITCHING y ROUTING

Para este caso se integran la configuración de VLAN en una red redundante y en un dominio VTP controlado mediante un switch capa 3. Adicionalmente, se habilita el enrutamiento y la redistribución de los protocolos RIP y OSPF. Finalmente, se configura la autenticación mediante un servidor Radius.

LABORATORIO N° 6: LISTAS DE CONTROL DE ACCESO

Se realizará la implementación básica y avanzada de la configuración EIGRP, aplicando listas de control de acceso para el filtro en la comunicación de diferentes servicios, de acuerdo a ciertos requerimientos de conexión.

LABORATORIO N° 7: VLAN Y RUTA DE RESPALDO CON CONEXIÓN INALAMBRICA

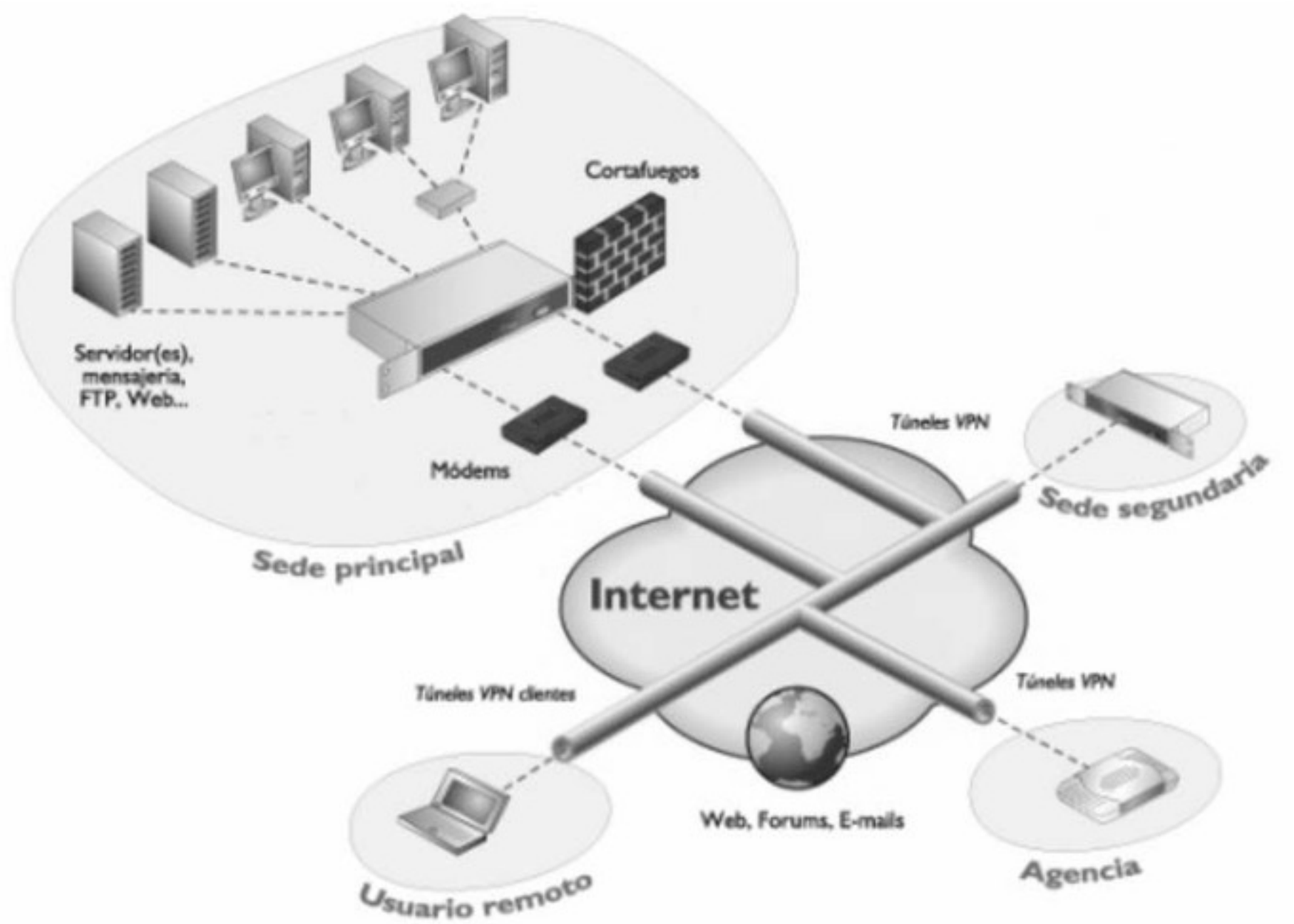
La topología realizada es la conexión de una red LAN con VLAN inalámbrica (WLAN), y una red WAN con enlace punto a punto de dos routers, que permite comunicar dos sucursales bajo EIGRP, al cual se le adiciona una ruta de respaldo inalámbrica con bridge Aironet. Así mismo, se habilita la autenticación de dispositivos en un servidor TACACS+.

LABORATORIO N° 8:

Es una topología donde se muestra un caso típico que presenta una empresa que tiene conexión a Internet, al diferenciarse las características de los servicios que presenta un router. Las soluciones planteadas tienen que ver con listas de control de acceso, VLAN, servicios de DHCP, NAT, Autenticación, entre otros.

LABORATORIO N° 9: Principios básicos de conmutación y enrutamiento intermedio

El laboratorio está desarrollado en base al requerimiento de una empresa. La finalidad es describir el proceso de enrutamiento OSPF en una topología de red, donde a su vez se implementa la configuración de VLAN bajo un dominio VTP y se brinda solución a exigencias de direccionamiento IP, entre otras opciones.



Capítulo

4 Casos de estudio

LABORATORIO N° 1

DESCRIPCIÓN

Es un protocolo de puerta de enlace interna o **IGP** (*Internal Gateway Protocol*) utilizado por los routers (enrutadores).

En la actualidad existen tres versiones diferentes de RIP, las cuales son:

- **RIPv1**: No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058.
- **RIPv2**: Soporta subredes, CIDR y VLSM. Soporta autentificación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada vía MD5. Su especificación está recogida en RFC 1723 y en RFC 2453.
- **RIPng**: RIP para IPv6. Su especificación está recogida en el RFC 2080.

También existe un RIP para IPX, que casualmente lleva el mismo acrónimo, pero no está directamente relacionado con el RIP para redes IP, ad-hoc.

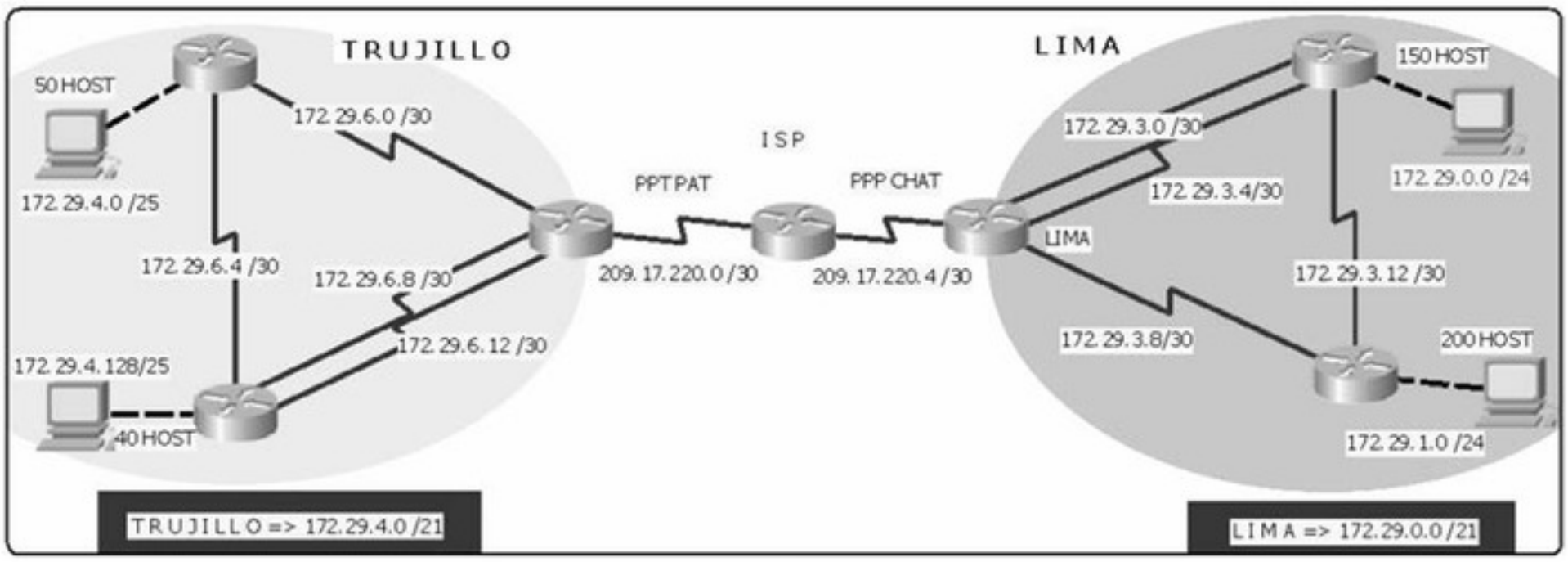
OBJETIVOS

- Configuración del protocolo RIP con la redistribución de rutas por defecto.

PLANTEAMIENTO

El escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

- Los routers Lima_2 y Trujillo_2 proporcionan el servicio DHCP a su propia red Lan y a los routers 3 de su ciudad.
- Configure PPP en los enlaces hacia el ISP, con autenticación.
- Habilite NAT de sobrecarga en los routers Lima_1 y Trujillo_1.



DESARROLLO

Considerando los laboratorios iniciales, se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo.

- Realizar las rutinas de diagnóstico y dejar listos los equipos para su configuración.
- Realizar la conexión física de los equipos en base a la topología de red.
- Habilite la opción de captura de texto en el emulador (Hyperterminal).

1. CONFIGURACIÓN DEL ENRUTAMIENTO

- Como se sabe, el protocolo RIP es de los más sencillos de trabajar. Para configurarlo sólo necesita declararse la red principal, desactivar la sumarizacion automática y habilitar la versión 2.

```
router rip
 version 2
  network 172.29.0.0
  no auto-summary
```

- Los routers Lima_1 y Trujillo deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de RIP.

```
ip route 0.0.0.0 0.0.0.0 209.17.220.2
!
router rip
 version 2
network 172.29.0.0
 default-information originate
 no auto-summary
```

- El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Lima y Trujillo. Para el caso se sumarizan las subredes de cada uno a /22.

```
ip route 172.29.0.0 255.255.252.0 209.17.220.1
ip route 172.29.4.0 255.255.252.0 209.17.220.5
```

2. TABLA DE ENRUTAMIENTO

- Se verifica la tabla de enrutamiento en cada router para comprobar las redes y sus rutas. Asimismo, verifique el balanceo de carga que presentan los routers.
- Obsérvese en los routers Trujillo_1 y Lima_1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

```
TRUJILLO_1#SH IP ROUTE
Gateway of last resort is 209.17.220.2 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:17, Serial0/0/0
R       172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:15, Serial0/1/1
                        [120/1] via 172.29.6.10, 00:00:15, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
R       172.29.6.4/30 [120/1] via 172.29.6.2, 00:00:17, Serial0/0/0
                      [120/1] via 172.29.6.14, 00:00:15, Serial0/1/1
                      [120/1] via 172.29.6.10, 00:00:15, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/0/1
C       172.29.6.12/30 is directly connected, Serial0/1/1
    209.17.220.0/30 is subnetted, 1 subnets
C       209.17.220.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.17.220.2
```

```
LIMA_1#sh ip route
Gateway of last resort is 209.17.220.6 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.29.0.0/24 [120/1] via 172.29.3.6, 00:00:01, Serial0/1/1
                      [120/1] via 172.29.3.2, 00:00:01, Serial0/0/1
R       172.29.1.0/24 [120/1] via 172.29.3.10, 00:00:06, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/1/0
R       172.29.3.12/30 [120/1] via 172.29.3.6, 00:00:01, Serial0/1/1
                       [120/1] via 172.29.3.2, 00:00:01, Serial0/0/1
                       [120/1] via 172.29.3.10, 00:00:06, Serial0/1/0
    209.17.220.0/30 is subnetted, 1 subnets
C       209.17.220.4 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.6
```

- Los routers Trujillo_2 y Lima_2 también presentan similares redes conectadas directamente y recibidas mediante RIP.

```
TRUJILLO_2#sh ip route
Gateway of last resort is 172.29.6.1 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.29.4.0/25 is directly connected, FastEthernet0/0
R       172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
R       172.29.6.8/30 [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
                      [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
R       172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
                       [120/1] via 172.29.6.6, 00:00:28, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:06, Serial0/0/0
```

```
LIMA_2#sh ip rout
Gateway of last resort is 172.29.3.9 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R      172.29.0.0/24 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
C      172.29.1.0/24 is directly connected, FastEthernet0/0
R      172.29.3.0/30 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
                     [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
R      172.29.3.4/30 [120/1] via 172.29.3.13, 00:00:23, Serial0/0/1
                     [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
C      172.29.3.8/30 is directly connected, Serial0/0/0
C      172.29.3.12/30 is directly connected, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
```

- Finalmente las tablas de los routers restantes permiten visualizar rutas redundantes para el caso de la ruta por defecto.

```
TRUJILLO_3#sh ip route
Gateway of last resort is 172.29.6.13 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R      172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:17, Serial0/0/1
C      172.29.4.128/25 is directly connected, FastEthernet0/0
R      172.29.6.0/30 [120/1] via 172.29.6.13, 00:00:16, Serial0/1/0
                     [120/1] via 172.29.6.5, 00:00:17, Serial0/0/1
                     [120/1] via 172.29.6.9, 00:00:16, Serial0/0/0
C      172.29.6.4/30 is directly connected, Serial0/0/1
C      172.29.6.8/30 is directly connected, Serial0/0/0
C      172.29.6.12/30 is directly connected, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:16, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:16, Serial0/0/0
```

```
LIMA_3#sh ip route
Gateway of last resort is 172.29.3.5 to network 0.0.0.0
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.29.0.0/24 is directly connected, FastEthernet0/0
R      172.29.1.0/24 [120/1] via 172.29.3.14, 00:00:01, Serial0/0/1
C      172.29.3.0/30 is directly connected, Serial0/0/0
C      172.29.3.4/30 is directly connected, Serial0/1/0
R      172.29.3.8/30 [120/1] via 172.29.3.5, 00:00:27, Serial0/1/0
                     [120/1] via 172.29.3.1, 00:00:27, Serial0/0/0
                     [120/1] via 172.29.3.14, 00:00:01, Serial0/0/1
C      172.29.3.12/30 is directly connected, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:27, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:27, Serial0/0/0
```

- El router ISP sólo indicará sus rutas estáticas adicionales a las directamente conectadas.

```
ISP#sh ip route
Gateway of last resort is not set
    172.29.0.0/22 is subnetted, 2 subnets
S      172.29.0.0 [1/0] via 209.17.220.5
S      172.29.4.0 [1/0] via 209.17.220.1
    209.17.220.0/30 is subnetted, 2 subnets
C      209.17.220.0 is directly connected, Serial0/0/0
C      209.17.220.4 is directly connected, Serial0/0/1
```

3. DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO RIP

- Con la finalidad de no propagar las publicaciones por interfaces que no lo requieran, se indican las interfaces de cada router que no requieren de su desactivación.

```
router rip
passive-interface Serial0/0/0
```

ROUTER	INTERFAZ
LIMA_1	SERIAL 0/0/1, 0/1/0, 0/1/1
LIMA_2	SERIAL 0/0/0, 0/0/1
LIMA_3	SERIAL 0/0/0, 0/0/1, 0/1/0
TRUJILLO_1	SERIAL 0/0/0, 0/0/1, 0/1/1
TRUJILLO_2	SERIAL 0/0/0, 0/0/1
TRUJILLO_3	SERIAL 0/0/0, 0/0/1, 0/1/0
ISP	No lo requiere

4. VERIFICACIÓN DEL PROTOCOLO RIP

- A manera de ejemplo se verifica sólo el router Trujillo_1, donde también se confirman las opciones configuradas, como el **passive interface** para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación, entre otros datos.

```
TRUJILLO_1#sh ip protocols
Routing Protocol is “rip”
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface         Send  Recv  Triggered RIP  Key-chain
  Serial0/1/1       2     2
  Serial0/0/0       2     2
  Serial0/0/1       2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     Serial0/1/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.6.2           120      00:00:01
     172.29.6.10          120      00:00:08
     172.29.6.14          120      00:00:08
Distance: (default is 120)
```

- Con el comando show ip rip database se muestra la base de dato de RIP, donde se informa de manera detallada de todas las rutas hacia cada red. Para el ejemplo, es el router Trujillo_3.

```
TRUJILLO_3#sh ip rip database
0.0.0.0/0
    [1] via 172.29.6.9, 00:00:10, Serial0/0/0
    [1] via 172.29.6.13, 00:00:10, Serial0/1/0
172.29.4.0/25
    [1] via 172.29.6.5, 00:00:01, Serial0/0/1
172.29.4.128/25    directly connected, FastEthernet0/0
172.29.6.0/30
    [1] via 172.29.6.5, 00:00:01, Serial0/0/1
    [1] via 172.29.6.9, 00:00:10, Serial0/0/0
    [1] via 172.29.6.13, 00:00:10, Serial0/1/0
172.29.6.4/30     directly connected, Serial0/0/1
172.29.6.8/30     directly connected, Serial0/0/0
172.29.6.12/30    directly connected, Serial0/1/0
```

5. CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

- Según el esquema, se requiere que el enlace Trujillo_1 con ISP sea configurado con autenticación PAT.

```
username TRUJILLO_1 password 0 seguridad123
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username ISP password 0 seguridad123
!
```

```
username ISP password 0 seguridad123
!
interface Serial0/1/0
encapsulation ppp
 ppp authentication pap
 ppp pap sent-username TRUJILLO_1 password 0 seguridad123
```

- El enlace Lima_1 con ISP se ha configurado con autenticación CHAT.

```
username ISP password 0 seguridad456
!
interface Serial0/0/0
encapsulation ppp
 ppp authentication chap
```

```
username LIMA_1 password 0 seguridad456
!
interface Serial0/0/1
encapsulation ppp
 ppp authentication chap
```

6. CONFIGURACION DE PAT

- En el escenario, si se activa NAT en cada equipo de salida (Trujillo_1 y Lima_1), los routers internos de una ciudad no podrán llegar hasta los router internos en el otro extremo, sólo existirá comunicación hasta los routers Lima_1, ISP y Trujillo_1.
- **Configuración de NAT en router Trujillo_1**. En una sentencia se indica que las direcciones de la lista de acceso 10 serán traducidas a la dirección de la interfaz serial 0/1/0.

```
ip nat inside source list 10 interface Serial0/1/0 overload
access-list 10 permit 172.29.4.0 0.0.3.255
```

- La traducción debe indicar las interfaces de entrada y de salida.

```
interface Serial0/0/0
ip nat inside
!
interface Serial0/0/1
ip nat inside
!
interface Serial0/1/0
ip nat outside
!
interface Serial0/1/1
ip nat inside
```

- Al realizar la prueba de ping (icmp), automáticamente la dirección es traducida a la dirección de la interfaz serial 0/1/0 del router Trujillo_1, con diferente puerto.

```
TRUJILLO_1# sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.1:2    172.29.4.130:2     209.17.220.2:2     209.17.220.2:2
icmp 209.17.220.1:8    172.29.6.14:8      209.17.220.2:8     209.17.220.2:8
icmp 209.17.220.1:4    172.29.6.2:4       209.17.220.2:4     209.17.220.2:4
```

- **Configuración de NAT en router Lima_1**. En una sentencia se indica que las direcciones de la lista de acceso 10 serán traducidas ala dirección de la interfaz serial 0/1/0.

```
ip nat inside source list 10 interface Serial0/1/0 overload
access-list 10 permit 172.29.0.0 0.0.3.255
```

- La traducción debe indicar las interfaces de entrada y de salida.

```
interface Serial0/0/0
ip nat outside
!
interface Serial0/0/1
ip nat inside
!
interface Serial0/1/0
ip nat inside
!
interface Serial0/1/1
ip nat inside
```

- Al realizar la prueba de ping (icmp), automáticamente la dirección es traducida a la dirección de la interfaz serial 0/1/0 del router Trujillo_1, con diferente puerto.

```
LIMA_1#SH IP NAT TRanslations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.5:1    172.29.3.10:1      209.17.220.2:1     209.17.220.2:1
icmp 209.17.220.5:2    172.29.3.10:2      172.29.6.1:2       172.29.6.1:2
icmp 209.17.220.5:1024 172.29.3.10:3      172.29.6.1:3       172.29.6.1:1024
icmp 209.17.220.5:3    172.29.3.2:3       209.17.220.2:3     209.17.220.2:3
```

7. CONFIGURACIÓN DEL SERVICIO DHCP

- Configuración de la red Trujillo_2 y Trujillo_3, donde el router Trujillo_2 debe ser el servidor DHCP para ambas redes Lan.

```
TRUJILLO_2#
ip dhcp excluded-address 179.29.4.129 172.29.4.133
ip dhcp excluded-address 179.29.4.1 172.29.4.5
!
ip dhcp pool DHCP-T3
 network 179.29.4.128 255.255.255.128
 default-router 179.29.4.128
ip dhcp pool DHCP-T2
 network 179.29.4.0 255.255.255.128
 default-router 179.29.4.1
```

- El router Trujillo_3 deberá habilitar el paso de los mensajes broadcast hacia el IP del router Trujillo_2.

```
TRUJILLO_3#sh run
!
!
interface FastEthernet0/0
ip helper-address 172.29.6.5
```

- Configuración de la red Lima_2 y Lima_3, donde el router Trujillo_2 debe ser el servidor DHCP para ambas redes Lan.

```
LIMA_2#
ip dhcp excluded-address 179.29.0.1 172.29.0.5
ip dhcp excluded-address 179.29.1.1 172.29.1.5
!
ip dhcp pool DHCP-L3
 network 179.29.0.0 255.255.255.0
 default-router 179.29.0.1
ip dhcp pool DHCP-L2
 network 179.29.1.0 255.255.255.0
 default-router 179.29.1.1
```

- El router Lima deberá habilitar el paso de los mensajes broadcast hacia el IP del router Lima_2.

```
LIMA_3#sh run
!
!
interface FastEthernet0/0
ip helper-address 172.29.3.14
```

8. Configuración final de cada router

```
ISP#sh runn
!
!
username LIMA_1 password 0 seguridad456
username TRUJILLO_1 password 0 seguridad123
!
!
interface Serial0/0/0
 ip address 209.17.220.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username ISP password 0 seguridad123
!
interface Serial0/0/1
 ip address 209.17.220.6 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
!
ip classless
ip route 172.29.0.0 255.255.252.0 209.17.220.1
ip route 172.29.4.0 255.255.252.0 209.17.220.5
!
!
```

```
TRUJILLO_1#sh run
!
!
username ISP password 0 seguridad123
!
!
interface Serial0/0/0
 ip address 172.29.6.1 255.255.255.252
ip nat inside
!
interface Serial0/0/1
 ip address 172.29.6.9 255.255.255.252
ip nat inside
!
interface Serial0/1/0
 ip address 209.17.220.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username TRUJILLO_1 password 0 seguridad123
 ip nat outside
clock rate 64000
!
interface Serial0/1/1
 ip address 172.29.6.13 255.255.255.252
ip nat inside
 clock rate 64000
!
router rip
```

```
 version 2
 passive-interface Serial0/1/0
 network 172.29.0.0
 default-information originate
 no auto-summary
!
ip nat inside source list 10 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.2
!
!
access-list 10 permit 172.29.4.0 0.0.3.255
!
```

```
LIMA_1#sh runn
!
!
username ISP password 0 seguridad456
!
!
interface Serial0/0/0
 ip address 209.17.220.5 255.255.255.252
 encapsulation ppp
 ppp authentication chap
ip nat outside
!
interface Serial0/0/1
 ip address 172.29.3.1 255.255.255.252
 clock rate 64000
ip nat inside
!
interface Serial0/1/0
 ip address 172.29.3.9 255.255.255.252
 clock rate 64000
ip nat inside
!
interface Serial0/1/1
 ip address 172.29.3.5 255.255.255.252
ip nat inside
!
!
router rip
 version 2
 passive-interface Serial0/0/0
 network 172.29.0.0
 default-information originate
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.6
!
!
```

```
TRUJILLO_2#sh runn
!
!
interface FastEthernet0/0
 ip address 172.29.4.1 255.255.255.128
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.29.6.2 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.29.6.5 255.255.255.252
 clock rate 64000
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
!
ip classless
!
!
ip dhcp excluded-address 179.29.4.129 172.29.4.133
ip dhcp excluded-address 179.29.4.1 172.29.4.5
!
ip dhcp pool DHCP-T3
 network 179.29.4.128 255.255.255.128
 default-router 179.29.4.128
ip dhcp pool DHCP-T2
 network 179.29.4.0 255.255.255.128
 default-router 179.29.4.1
!
!
```

```
TRUJILLO_3#sh run
!
!
interface FastEthernet0/0
 ip address 172.29.4.129 255.255.255.128
 ip helper-address 172.29.6.5
duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.29.6.10 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.29.6.6 255.255.255.252
!
interface Serial0/1/0
 ip address 172.29.6.14 255.255.255.252
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
```

```
LIMA_3#sh runn
!
!
interface FastEthernet0/0
 ip address 172.29.0.1 255.255.255.0
 ip helper-address 172.29.3.14
duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.29.3.2 255.255.255.252
!
interface Serial0/0/1
 ip address 172.29.3.13 255.255.255.252
 clock rate 64000
!
interface Serial0/1/0
 ip address 172.29.3.6 255.255.255.252
 clock rate 64000
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
!
```

```
LIMA_2#sh run
!
!
interface FastEthernet0/0
 ip address 172.29.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.29.3.10 255.255.255.252
!
interface Serial0/0/1
 ip address 172.29.3.14 255.255.255.252
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 172.29.0.0
 no auto-summary
!
ip classless
!
!
ip dhcp excluded-address 179.29.0.1 172.29.0.5
ip dhcp excluded-address 179.29.1.1 172.29.1.5
!
ip dhcp pool DHCP-L3
 network 179.29.0.0 255.255.255.0
 default-router 179.29.0.1
ip dhcp pool DHCP-L2
 network 179.29.1.0 255.255.255.0
 default-router 179.29.1.1

!
```

CONCLUSIONES

_____

_____

_____

TAREAS

- Habilite la autenticación RIP.
- Modifique el balanceo de carga en los routers Lima_3 y Trujillo_3.
- Habilite el enrutamiento OSPF en los routers de Lima y EIGRP, en los routers de Trujillo.

LABORATORIO N° 2

INTRODUCCIÓN

La integración de diversos servicios en una red facilita su funcionalidad, permitiendo cumplir los requerimientos de operación. Por ello se necesita modificar paulatinamente el escenario y presentar diferentes alternativas que solucionen las exigencias y planteen configuraciones adicionales en caso que el sistema falle.

OBJETIVO

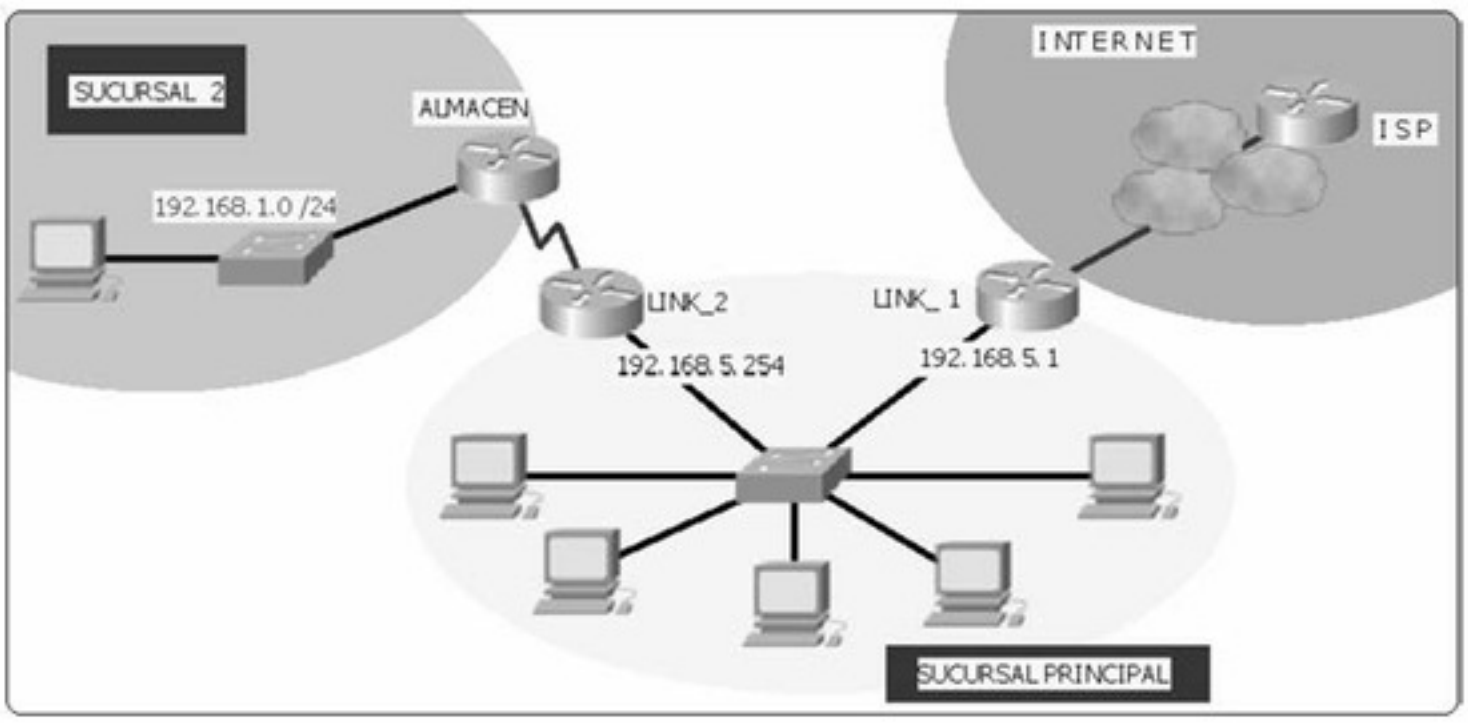
- Implementación de diversos servicios como solución en una conexión de red.

DESCRIPCIÓN

Los siguientes escenarios de red presentan cierta similitud, en ellos se tiene una conexión hacia Internet y otra hacia una sucursal.

Se aplican, a su vez, situaciones, casos prácticos donde se modifica parte de la configuración para la implementación de VLAN, PAT, encapsulamiento Frame Relay, enrutamiento estático, enrutamiento EIGRP, entre otras configuraciones.

CASO 1: ENRUTAMIENTO ESTÁTICO EN UNA CONEXIÓN WAN CON ENCAPSULAMIENTO HDLC.



FASE 1: CONEXIÓN DE LA RED PRINCIPAL HACIA INTERNET

TAREAS:

- Habilitar una ruta por defecto hacia Internet en el router LINK_1.
- Habilitar el servicio DHCP en el router LINK_1 hacia la red Lan.
- Configuración de una ruta estática en el router ISP hacia la red Lan.
- Todos los Hosts de la red Lan tendrán como Gateway al router LINK_1.

DESARROLLO:

1. En la configuración del router LINK_1 se observa:
   - La ruta agregada por defecto.
   - El servicio DHCP con el pool DUAL, donde se excluyen de la asignación las direcciones 192.168.5.1 y 192.168.5.254, ya que pertenecen a los routers LINK_1 y LINK_2.

```
LINK_1#SH RUNN
!
hostname LINK_1
!
ip ssh version 1
!
interface FastEthernet0/0
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.0
 clock rate 64000
……<resultado omitido>……..
!
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
ip dhcp excluded-address 192.168.5.254
ip dhcp excluded-address 192.168.5.1
!
ip dhcp pool DUAL
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
 dns-server 200.62.191.11
!
```

2. Se presenta a continuación la configuración del router ISP, donde se observa que se han creado dos interfaces loopback con la finalidad de representar servidores en Internet.

```
ISP#SH RUN
!
hostname ISP
!
ip ssh version 1
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback1
 ip address 172.16.2.1 255.255.255.0
!
```

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 202.2.2.2 255.255.255.0
!
ip route 192.168.5.0 255.255.255.0 202.2.2.1
!
```

3. Se verifica la tabla de enrutamiento en cada router, donde se observan las rutas estáticas agregadas (resaltadas en negrita), así como las redes directamente conectadas.
4. En el router LINK-1, la ruta por defecto:

```
LINK_1#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
C    202.2.2.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 is directly connected, Serial0/0
LINK_1#
```

5. En el router ISP, la ruta estática hacia la red interna:

```
ISP#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback1
S    192.168.5.0/24 [1/0] via 202.2.2.1
C    202.2.2.0/24 is directly connected, Serial0/0
```

6. Se verifica en uno de los Hosts de la red interna si recibe la configuración de direcciones IP del servidor DHCP (router LINK_1).

```
Adaptador de Ethernet Conexión de área local:
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Marvell Yukon 88E8039 PCI-E Fast Ethernet Controller
 Dirección física. . . . . . . . . . . . . . : 00-1D-72-58-19-85
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.5.2(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.5.1
   Servidores DNS. . . . . . . . . . . . . . : 200.62.191.11
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

7. Se realiza la prueba de conectividad hacia la puerta de enlace y a la dirección IP de la interfaz loopback del router ISP.

```
C:\Users\hector>ping 192.168.5.1
Haciendo ping a 192.168.5.1 con 32 bytes de datos:
Respuesta desde 192.168.5.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.5.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.5.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.5.1: bytes=32 tiempo=1ms TTL=64
Estadísticas de ping para 192.168.5.1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 1ms, Máximo = 4ms, Media = 1ms

C:\Users\hector>ping 172.16.1.1
Haciendo ping a 172.16.1.1 con 32 bytes de datos:
Respuesta desde 172.16.1.1: bytes=32 tiempo=36ms TTL=57
Respuesta desde 172.16.1.1:bytes=32 tiempo=43ms TTL=57
Respuesta desde 172.16.1.1:bytes=32 tiempo=42ms TTL=57
Respuesta desde 172.16.1.1:bytes=32 tiempo=41ms TTL=57
Estadísticas de ping para 172.16.1.1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 36ms, Máximo = 43ms, Media = 40ms
```

FASE 2: CONEXIÓN DE SUCURSAL 2 HACIA SUCURSAL PRINCIPAL

TAREAS:

- Establecer una ruta estática en el router LINK_1 para alcanzar la red Lan de sucursal 2.
- El router LINK_2 deberá tener también una ruta estática hacia la red Lan de la sucursal 2.
- El router en la sucursal deberá contar con una ruta estática que le permita llegar a la red Lan de la sucursal principal.
- La red Lan de la nueva sucursal no tendrá salida a Internet.

DESARROLLO:

1. Se debe tener presente que tanto el router LINK_2 como el router LINK_1 pueden trabajar como puertas de enlace, ya que ambos deberán contar con las rutas dirigidas tanto a Internet como a la red de la sucursal 2.
2. En la configuración del router LINK_1 se muestra el agregado de la ruta estática dirigida a la sucursal 2.

```
LINK_1#SH RUNN
!
……<resultado omitido>……..
!
ip route 192.168.1.0 255.255.255.0 192.168.5.254
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
```

3. Observar que la ruta estática agregada indica que para alcanzar la red 192.168.1.0 deberán enviarse los paquetes a la dirección IP de la FastEthernet del router LINK_2.
4. Es decir que si un Host de la red principal intenta llegar a la red 192.168.1.0, el paquete será enviado al router LINK_1, para luego regresar a la red mediante el switch y llegar al router LINK_2, el cual lo enrutará hacia dicho destino.
5. En la tabla de enrutamiento del router LINK_1 se muestran las rutas identificadas, donde se resalta la nueva ruta estática.

```
LINK_1#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S    192.168.1.0/24 [1/0] via 192.168.5.254
C    192.168.5.0/24 is directly connected, FastEthernet0/0
C    202.2.2.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 is directly connected, Serial0/0
LINK_1#
```

6. En la configuración del router LINK_2 observamos que se agrega la ruta estática, dirigida a la sucursal 2, mediante su interfaz serial.

```
LINK_2#SH RUN
!
hostname LINK_2
!
ip ssh version 1
!
interface FastEthernet0/0
 ip address 192.168.5.254 255.255.255.0
 duplex auto
 speed auto
!
……..
!
interface Serial0/0
 ip address 200.1.1.1 255.255.255.0
!
ip route 192.168.1.0 255.255.255.0 Serial0/0
!
```

7. En la tabla de enrutamiento del router LINK_2 se muestran las rutas identificadas, resaltándose la nueva ruta estática.

```
LINK_2#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is not set
S    192.168.1.0/24 is directly connected, Serial0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
C    200.1.1.0/24 is directly connected, Serial0/0
```

8. En la configuración del router ALMACÉN observamos que se agrega la ruta estática, dirigida a la sucursal principal (red 192.168.5.0) mediante su interfaz serial.

```
ALMACÉN#sh runn
!
hostname ALMACÉN
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.1.1.2 255.255.255.0
 clock rate 64000
!
ip route 192.168.5.0 255.255.255.0 Serial0/0
!
```

9. En la tabla de enrutamiento del router ALMACÉN se muestran las rutas identificadas, resaltándose la nueva ruta estática.

```
ALMACÉN#sh ip route
……<resultado omitido>……..
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.5.0/24 is directly connected, Serial0/0
C    200.1.1.0/24 is directly connected, Serial0/0
ALMACÉN#
```

10. Se verifica en uno de los Hosts de la red, en la sucursal 2, la configuración de direcciones IP.
11. Se realiza posteriormente la prueba de conectividad hacia la puerta de enlace y hacia un Host de la red principal.

```
Adaptador de Ethernet Conexión de área local:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.2
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

FASE 3: CONEXIÓN DE SUCURSAL 2 HACIA SUCURSAL PRINCIPAL E INTERNET

DESARROLLO:

1. Para permitir que la red de la sucursal 2 acceda a Internet deberemos agregar las siguientes rutas por defecto, tanto en el router ALMACÉN como en el router LINK_2, sin necesidad de modificar su configuración.

```
ALMACÉN(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.1
```

```
LINK_2(config)#ip route 0.0.0.0 0.0.0.0 192.168.5.1
```

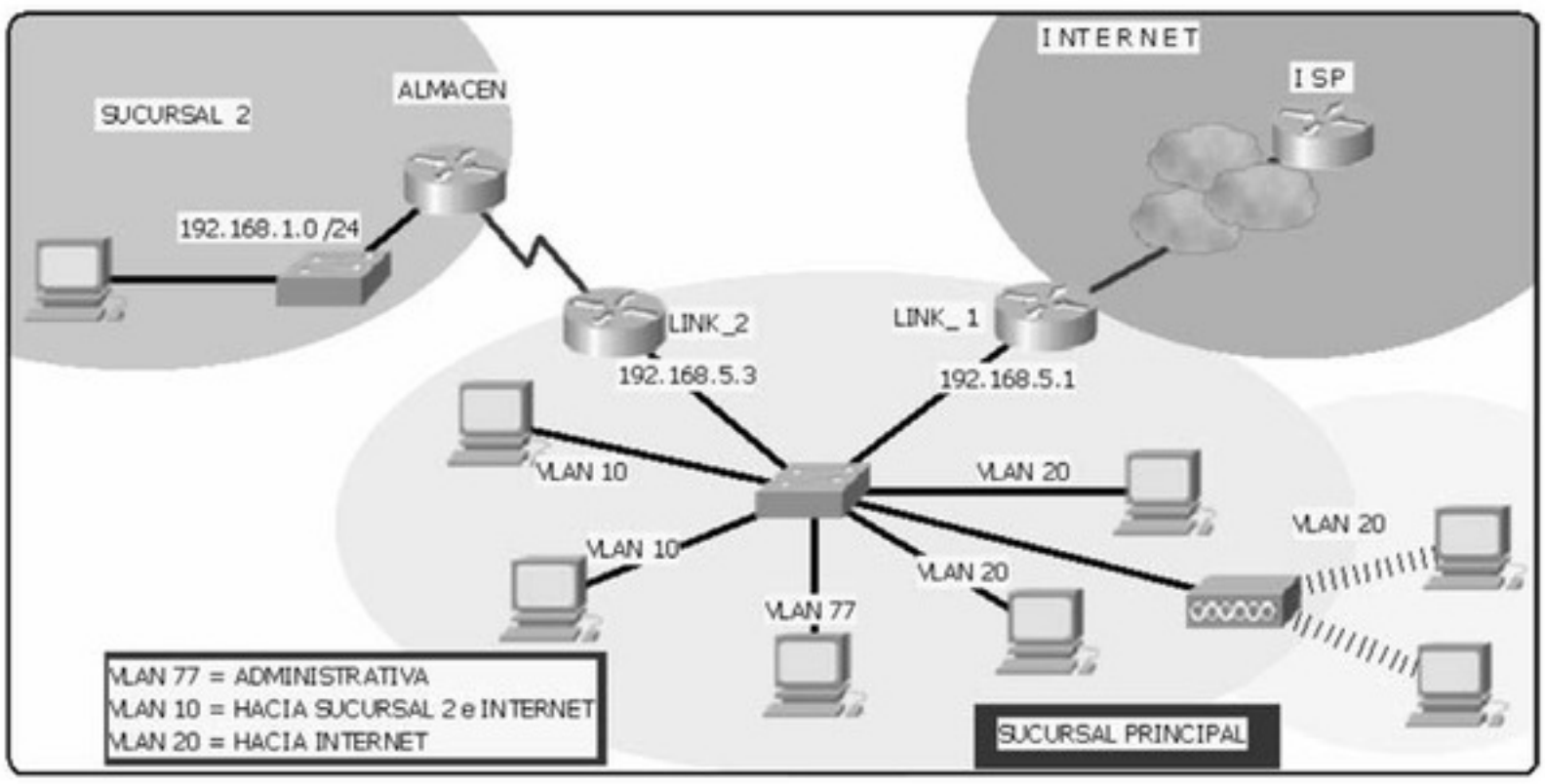
2. El router ISP debe tener una ruta estática dirigida a la red sucursal 2 para facilitar la ubicación de la red y el retorno de paquetes desde los servidores externos.

```
ISP(config)#ip route 192.168.1.0 255.255.255.0 202.2.2.1
```

3. A continuación se realiza la prueba de conectividad desde un Host de la red en la sucursal 2 hacia la interfaz loopback del router ISP.

```
C:\Users\hector>ping 172.16.1.1
Haciendo ping a 172.16.1.1 con 32 bytes de datos:
Respuesta desde172.16.1.1: bytes=32 tiempo=265ms TTL=116
Respuesta desde172.16.1.1: bytes=32 tiempo=195ms TTL=116
Respuesta desde 172.16.1.1: bytes=32 tiempo=193ms TTL=116
Respuesta desde 172.16.1.1: bytes=32 tiempo=196ms TTL=116
Estadísticas de ping para 172.16.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 193ms, Máximo = 265ms, Media = 212ms
```

CASO 2: RED PRINCIPAL CON VLAN Y CONEXIÓN INALÁMBRICA.



FASE 1: CONFIGURACIÓN DEL SWITCH:

TAREAS:

- Agregar la VLAN 10, 20, 77 y definir los puertos a emplear.
- Definir la VLAN 77 como VLAN nativa y administrativa.
- Definir los enlaces troncales.

- Indicar las VLAN que circulan por los enlaces troncales.
- La VLAN 20 no debe tener comunicación hacia la red de la sucursal 2.

DESARROLLO:

1. En el switch de la red principal se definen todas las características antes mencionadas, considerando además:
   - Habilitar el puerto 24 para la VLAN 77, para una posible administración.
   - Deshabilitar los puertos no empleados.
2. Los puertos 1 y 2 se han configurado como enlaces troncales al tener conexión con los routers LINK_1 y LINK_2; asimismo, vienen indicándose las VLAN soportadas.
3. Para el caso, los puertos 3 y 4 se han definido para la VLAN 10 y los puertos 5 y 6, para la VLAN 20.
4. El puerto 24 está establecido como acceso para la VLAN administrativa.
5. El switch tiene definida la nueva VLAN nativa como VLAN 77, con la dirección 192.168.5.2 /26.
6. El switch tendrá el Gateway por defecto a la dirección 192.168.5.1 que corresponde al IP del router LINK_1.

```
Switch#SH RUN
hostname Switch
!
!
interface FastEthernet0/1
 switchport trunk native vlan 77
 switchport trunk allowed vlan 10,77
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 77
 switchport trunk allowed vlan 10,20,77
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
……<resultado omitido>……..
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport access vlan 77
```

```
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan77
 ip address 192.168.5.2 255.255.255.192
!
ip default-gateway 192.168.5.1
!
```

FASE 2: CONFIGURACIÓN DEL ROUTER LINK_1:

TAREAS:

1. Habilitar subinterfaces para intervlan.
2. Definir las subredes en cada subinterfaz.
3. Configurar el servicio DHCP para cada VLAN.
4. Modificar el enrutamiento estático.

DESARROLLO:

1. La configuración del router LINK_1 se ha mantenido en cuanto a su enrutamiento, aunque sólo presenta la modificación de la ruta estática hacia la red 192.168.1.0 /24.
   - Como el router LINK_2 modificó su IP en la red principal, ahora la ruta estática indica esa dirección (192.168.5.3) como próximo salto.
   - La ruta por defecto no requiere de modificación.
2. Se han agregado tres subinterfaces que corresponden a las VLAN 10, 20 y 77, respectivamente, donde se han definido tres subredes de 62 Hosts cada una.
3. Recordar que la VLAN 77, al ser definida en su encapsulamiento, debe indicar que será la nativa.
4. Finalizando la configuración del router, se define la configuración DHCP para cada una de la VLAN, asimismo, una lista de direcciones que no serán asignadas a los clientes.

```
LINK_1#sh run
!
hostname LINK_1
!
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.5.65 255.255.255.192
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
```

```
 ip address 192.168.5.129 255.255.255.192
!
interface FastEthernet0/0.3
 encapsulation dot1Q 77 native
 ip address 192.168.5.1 255.255.255.192
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.0
 clock rate 64000
!
……<resultado omitido>……..
!
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 192.168.1.0 255.255.255.0 192.168.5.3
!
!
ip dhcp excluded-address 192.168.5.1 192.168.5.3
ip dhcp excluded-address 192.168.5.65 192.168.5.66
ip dhcp excluded-address 192.168.5.129 192.168.5.130
!
ip dhcp pool DUAL10
 network 192.168.5.64 255.255.255.192
 default-router 192.168.5.65
 dns-server 200.62.191.11
ip dhcp pool DUAL20
 network 192.168.5.128 255.255.255.192
 default-router 192.168.5.129
 dns-server 200.62.191.11
ip dhcp pool DUAL77
 network 192.168.5.0 255.255.255.192
 default-router 192.168.5.1
 dns-server 200.62.191.11
!
```

5. La tabla de enrutamiento indica las direcciones a cada red, tanto a Internet con su ruta por defecto y la ruta hacia la red sucursal 2; asimismo, indica las direcciones a las subredes directamente conectadas de cada VLAN.

```
LINK_1#sh ip route
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S    192.168.1.0/24 [1/0] via 192.168.5.3
     192.168.5.0/26 is subnetted, 3 subnets
C       192.168.5.0 is directly connected, FastEthernet0/0.3
C       192.168.5.64 is directly connected, FastEthernet0/0.1
C       192.168.5.128 is directly connected, FastEthernet0/0.2
C    202.2.2.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 is directly connected, Serial0/0
LINK_1#
```

FASE 3: CONFIGURACIÓN DEL ROUTER LINK_2:

TAREAS:

- Habilitar subinterfaces para intervlan de VLAN 10 y VLAN 77.
- Definir las subredes en cada subinterfaz.

DESARROLLO:

1. La configuración del router LINK_2 se ha mantenido en cuanto a su enrutamiento y dirección de interfaz serial.
2. Se han agregado dos subinterfaces que corresponden a las VLAN 10 y 77, que se han integrado a las subredes definidas anteriormente.
3. El caso indica que la VLAN 20 no deberá comunicarse con la sucursal 2, por lo que no se define una subinterfaz para esta VLAN.
4. Recordar que la VLAN 77 también deberá indicar en su encapsulamiento que será la nativa.

```
LINK_2#sh run
!
hostname LINK_2
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.5.66 255.255.255.192
!
interface FastEthernet0/0.3
 encapsulation dot1Q 77 native
 ip address 192.168.5.3 255.255.255.192
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.1.1.1 255.255.255.0
!
……<resultado omitido>……..
!
ip classless
ip route 192.168.1.0 255.255.255.0 Serial0/0
ip route 0.0.0.0 0.0.0.0 192.168.5.1
!
```

5. La tabla de enrutamiento en este router está modificada con respecto a las subinterfaces agregadas y que están dentro de subredes.

```
LINK_2# sh ip route
……<resultado omitido>……..
Gateway of last resort is 192.168.5.1 to network 0.0.0.0
S   192.168.1.0/24 is directly connected, Serial0/0
    192.168.5.0/26 is subnetted, 2 subnets
C      192.168.5.0 is directly connected, FastEthernet0/0.3
C      192.168.5.64 is directly connected, FastEthernet0/0.1
C   200.1.1.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 192.168.5.1
```

6. Los routers ALMACÉN e ISP no modifican su configuración con respecto del caso anterior, ya que la red principal mantiene su dirección de red 192.168.5.0 /24, que vendría a ser la dirección sumarizada de las subredes, con excepción de la subred 192.168.5.192 /26 que está reservada para un uso futuro.

FASE 4: PRUEBA:

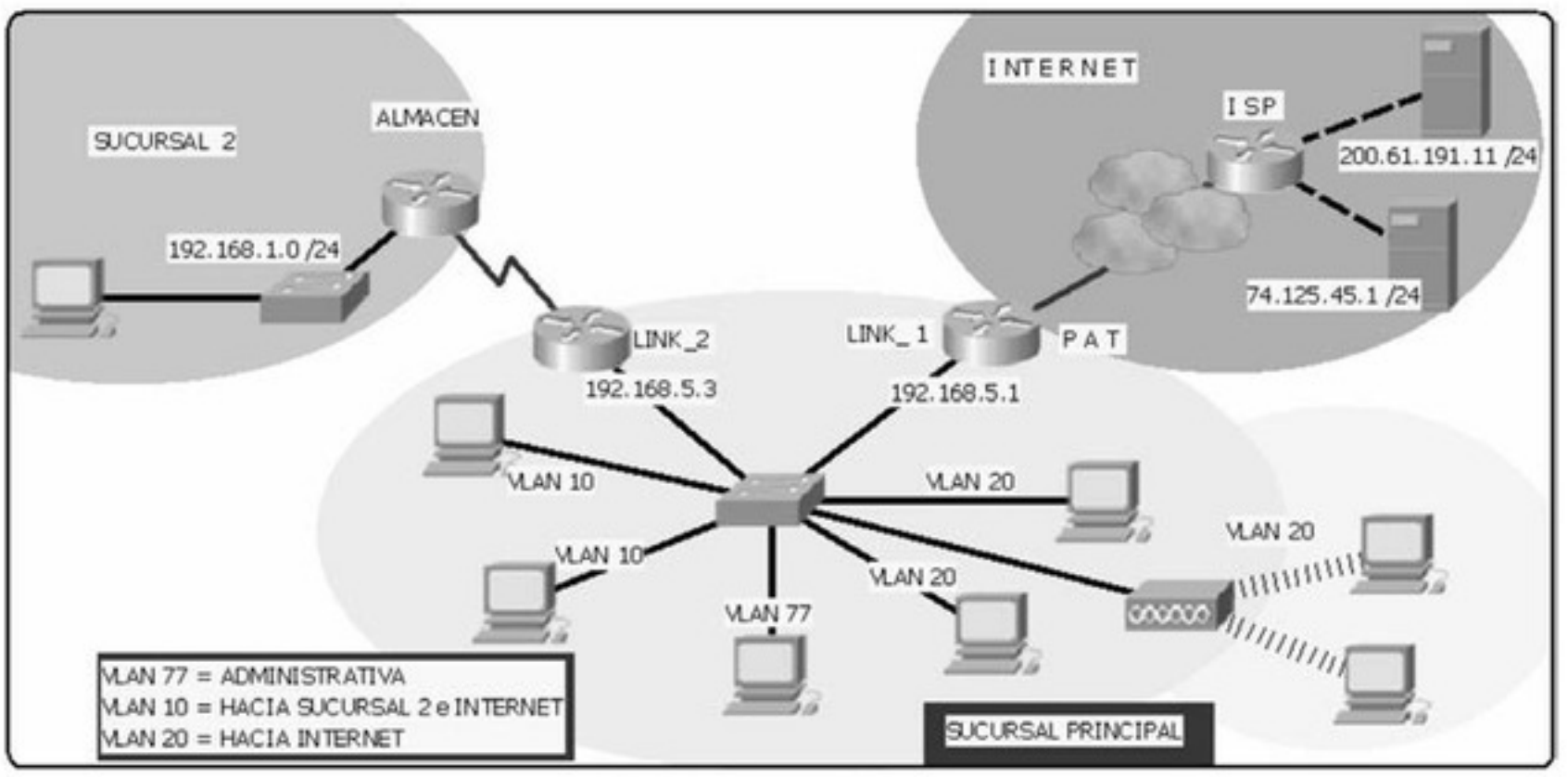
1. Se realiza posteriormente la prueba de conectividad de la red principal hacia un Host, desde la Lan de la sucursal 2.

```
C:\>ping 192.168.5.2
Haciendo ping a 192.168.5.2 con 32 bytes de datos:
Respuesta desde 192.168.5.2: bytes=32 tiempo=184ms TTL=55
Respuesta desde 192.168.5.2: bytes=32 tiempo=134ms TTL=55
Respuesta desde 192.168.5.2: bytes=32 tiempo=128ms TTL=55
Respuesta desde 192.168.5.2: bytes=32 tiempo=166ms TTL=55
Estadísticas de ping para 192.168.5.2:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 128ms, Máximo = 184ms, Media = 153ms
```

2. A continuación se realiza la prueba de conectividad desde un Host de la red principal hacia la interfaz loopback del router ISP.

```
C:\Users\hector>ping 172.16.1.1
Haciendo ping a 172.16.1.1 con 32 bytes de datos:
Respuesta desde172.16.1.1: bytes=32 tiempo=265ms TTL=116
Respuesta desde172.16.1.1: bytes=32 tiempo=195ms TTL=116
Respuesta desde 172.16.1.1: bytes=32 tiempo=193ms TTL=116
Respuesta desde 172.16.1.1: bytes=32 tiempo=196ms TTL=116
Estadísticas de ping para 172.16.1.1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 193ms, Máximo = 265ms, Media = 212ms
```

CASO 3: IMPLEMENTACIÓN DE PAT (NAT DE SOBRECARGA)



A diferencia de los casos anteriores, la red implementada podrá conectarse a Internet, donde el router ISP representa al equipo del proveedor de servicios, que puede tener un enrutamiento estático o dinámico hacia Internet.

La configuración en los routers ALMACÉN y LINK_2 no requiere de modificación, ya que el servicio NAT solo necesita ser implementado en el router LINK_1.

FASE 1: CONFIGURACIÓN DEL ROUTER ISP:

TAREAS:

- Deshabilitar la ruta estática hacia las redes 192.168.1.0 /24 y 192.168.5.0 /24.
- Habilitar el enrutamiento dinámico mediante OSPF, suponiendo que se requiere ello para su comunicación con los routers de Internet.

DESARROLLO:

1. La configuración del router ISP, si tiene contacto con otros routers de Internet, estará comunicando mediante el enrutamiento OSPF, al cual se agregan sus redes.
2. Esta configuración en realidad no tendrá relevancia para la comunicación de la red principal o la red de la sucursal 2.

```
ISP#sh run
!
hostname ISP
!
!
ip ssh version 1
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback1
 ip address 172.16.2.1 255.255.255.0
!
```

```
interface FastEthernet0/0
 ip address 200.62.191.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 74.125.45.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 202.2.2.2 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 202.2.2.0 0.0.0.255 area 0
 network 200.56.34.0 0.0.0.3 area 0
!
```

FASE 2: CONFIGURACIÓN DEL ROUTER LINK_1:

TAREAS:

- Habilitar PAT (NAT de sobrecarga).
- Mantener la configuración del caso anterior, incluyendo el direccionamiento y enrutamiento.

DESARROLLO:

1. El servicio de PAT requiere de:
   a. Una lista de control de acceso que incluya la red 192.168.1.0 y la red 192.168.5.0.
   b. Crear la relación entre la ACL 10 y el servicio PAT, donde se indique además la interfaz que será empleada para la traducción, en este caso, la interfaz serial 0/0.
   c. Definir la interfaz FastEthernet 0/0 como entrada y la interfaz serial 0/0, como salida.

```
LINK_1#SH RUN
!
hostname LINK_1
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.5.65 255.255.255.192
!
interface FastEthernet0/0.2
```

```
 encapsulation dot1Q 20
 ip address 192.168.5.129 255.255.255.192
!
interface FastEthernet0/0.3
 encapsulation dot1Q 77 native
 ip address 192.168.5.1 255.255.255.192
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.0
 ip nat outside
 clock rate 64000
!
!
ip nat inside source list 10 interface Serial0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 192.168.1.0 255.255.255.0 192.168.5.3
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 10 permit 192.168.1.0 0.0.0.255
!
ip dhcp excluded-address 192.168.5.1 192.168.5.3
ip dhcp excluded-address 192.168.5.65 192.168.5.66
ip dhcp excluded-address 192.168.5.129 192.168.5.130
!
ip dhcp pool DUAL10
 network 192.168.5.64 255.255.255.192
 default-router 192.168.5.65
 dns-server 200.62.191.11
ip dhcp pool DUAL20
 network 192.168.5.128 255.255.255.192
 default-router 192.168.5.129
 dns-server 200.62.191.11
ip dhcp pool DUAL77
 network 192.168.5.0 255.255.255.192
 default-router 192.168.5.1
 dns-server 200.62.191.11
!
```

FASE 3: PRUEBA:

TAREAS:

- Comprobación de asignación de direcciones mediante DHCP.
- Prueba de conectividad hacia dominios en Internet.

DESARROLLO:

1. Verificamos la dirección asignada por el servidor DHCP hacia un Host de la red principal.

```
Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . :
  Descripción . . . . . . . . . . . . . . . : Marvell Yukon 88E8039 PCI-E Fast Ethernet Controller
 Dirección física. . . . . . . . . . . . . : 00-1D-72-58-19-85
  DHCP habilitado . . . . . . . . . . . . . : no
  Configuración automática habilitada . . . : sí
  Dirección IPv4. . . . . . . . . . . . . . : 192.168.5.2(Preferido)
  Máscara de subred . . . . . . . . . . . . : 255.255.255.192
  Puerta de enlace predeterminada . . . . . : 192.168.5.132
  Servidores DNS. . . . . . . . . . . . . . : 200.62.191.11
  NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

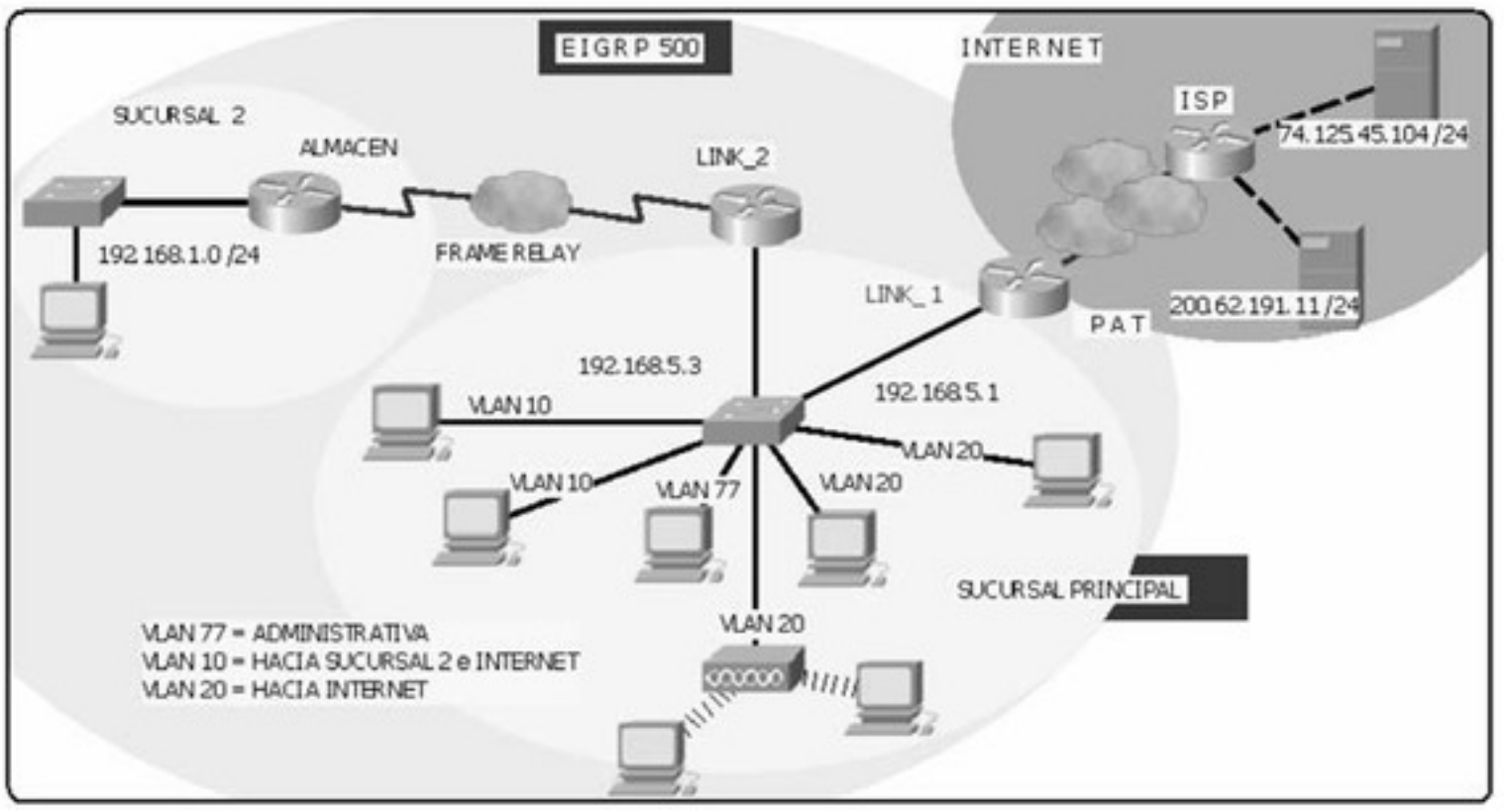
2. Se realiza la prueba de conectividad a algunos dominios de Internet.

```
C:\Users\hector>ping www.google.com
Haciendo ping a www.l.google.com [74.125.45.104] con 32 bytes de datos:
Respuesta desde 74.125.45.104: bytes=32 tiempo=171ms TTL=55
Respuesta desde 74.125.45.104: bytes=32 tiempo=126ms TTL=55
Respuesta desde 74.125.45.104: bytes=32 tiempo=129ms TTL=55
Respuesta desde 74.125.45.104: bytes=32 tiempo=133ms TTL=55
Estadísticas de ping para 74.125.45.104:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 126ms, Máximo = 171ms, Media = 139ms
C:\Users\hector>ping www.telmex.com
Haciendo ping a www.telmex.com [200.57.141.200] con 32 bytes de datos:
Respuesta desde 200.57.141.200: bytes=32 tiempo=265ms TTL=116
Respuesta desde 200.57.141.200: bytes=32 tiempo=195ms TTL=116
Respuesta desde 200.57.141.200: bytes=32 tiempo=193ms TTL=116
Respuesta desde 200.57.141.200: bytes=32 tiempo=196ms TTL=116
Estadísticas de ping para 200.57.141.200:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 193ms, Máximo = 265ms, Media = 212ms
```

3. Se revisa la tabla de traducción NAT en el router LINK_1, donde se indican los diversos protocolos que se están empleando, así como las direcciones internas y la traducción respectiva con su número de puerto de la interfaz serial 0/0.

```
LINK_1#SH IP NAT TRanslations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.2.2.1:24      192.168.1.2:24     202.2.2.2:24       202.2.2.2:24
icmp 202.2.2.1:1024    192.168.5.131:5    202.2.2.2:5        202.2.2.2:1024
icmp 202.2.2.1:6       192.168.5.135:6    202.2.2.2:6        202.2.2.2:6
icmp 202.2.2.1:35      192.168.5.4:35     202.2.2.2:35       202.2.2.2:35
icmp 202.2.2.1:16      192.168.5.67:16    202.2.2.2:16       202.2.2.2:16
icmp 202.2.2.1:74      192.168.5.68:74    202.2.2.2:74       202.2.2.2:74
icmp 202.2.2.1:11      192.168.5.132:11   74.125.45.104:11   74.125.45.104:11
icmp 202.2.2.1:12      192.168.5.132:12   74.125.45.104:12   74.125.45.104:12
icmp 202.2.2.1:13      192.168.5.132:13   74.125.45.104:13   74.125.45.104:13
icmp 202.2.2.1:14      192.168.5.132:14   74.125.45.104:14   74.125.45.104:14
udp 202.2.2.1:1025     192.168.5.132:1025 200.62.191.11:53   200.62.191.11:53
udp 202.2.2.1:1026     192.168.5.132:1026 200.62.191.11:53   200.62.191.11:53
tcp 202.2.2.1:1025     192.168.5.132:1025 74.125.45.104:80   74.125.45.104:80
```

CASO 4: IMPLEMENTACIÓN DEL ENRUTAMIENTO DINÁMICO CON EIGRP Y FRAME RELAY.



La configuración pretende modificar el enrutamiento estático y establecer el AS 500 mediante el protocolo EIGRP, por lo que el enrutamiento estático se mantendrá como un enrutamiento de respaldo para comunicar las dos sucursales.

Se necesita adicionalmente implementar la conexión entre los routers ALMACÉN y LINK_2, mediante una nube NBMA con encapsulamiento Frame Relay, la cual se presentó implementada en el capítulo de conexiones WAN y podría ser utilizada para completar el laboratorio.

Con respecto al caso anterior, el router ISP no modifica su configuración; para el caso de los siguientes routers, se presentan a continuación sus parámetros configurados:

FASE 1: CONFIGURACIÓN DE ROUTER LINK_1:

TAREAS:

- Enrutamiento EIGRP en el AS 500.
- Modificar la distancia administrativa de la ruta estática hacia la sucursal 2.
- Redistribución de la ruta por defecto en el enrutamiento EIGRP.

DESARROLLO:

1. La configuración muestra que sólo se habilitó el enrutamiento EIGRP en el AS 500, donde sólo se declaran las subredes de la VLAN 10 y 77; la VLAN 20 no lo requiere ya que sólo accederá hacia Internet.
2. Dentro del enrutamiento EIGRP se redistribuye la ruta por defecto.
3. Como se requiere de una ruta estática de respaldo entre las sucursales, se modificó la distancia administrativa de la ruta hacia la red 192.168.1.0 /24 a un valor de 180 (mayor que la de EIGRP).

```
LINK_1#SH RUNN
!
hostname LINK_1
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
```

```
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.5.65 255.255.255.192
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.5.129 255.255.255.192
!
interface FastEthernet0/0.3
 encapsulation dot1Q 77 native
 ip address 192.168.5.1 255.255.255.192
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.0
 ip nat outside
 clock rate 64000
!
!
router eigrp 500
 redistribute static
 network 192.168.5.0 0.0.0.63
 network 192.168.5.64 0.0.0.63
 no auto-summary
!
ip nat inside source list 10 interface Serial0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 192.168.1.0 255.255.255.0 192.168.5.3 180
!
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 10 permit 192.168.1.0 0.0.0.255
!
ip dhcp excluded-address 192.168.5.1 192.168.5.3
ip dhcp excluded-address 192.168.5.65 192.168.5.66
ip dhcp excluded-address 192.168.5.129 192.168.5.130
!
ip dhcp pool DUAL10
 network 192.168.5.64 255.255.255.192
 default-router 192.168.5.65
 dns-server 200.62.191.11
ip dhcp pool DUAL20
 network 192.168.5.128 255.255.255.192
 default-router 192.168.5.129
 dns-server 200.62.191.11
ip dhcp pool DUAL77
 network 192.168.5.0 255.255.255.192
 default-router 192.168.5.1
 dns-server 200.62.191.11
!
```

4. La tabla de enrutamiento en el router muestra que mediante el enrutamiento EIGRP es posible alcanzar las redes 192.168.1.0/24 y 200.1.1.0 /24.

```
LINK_1#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0
D   192.168.1.0/24 [90/2174976] via 192.168.5.3, 00:11:30, FastEthernet0/0.3
    192.168.5.0/26 is subnetted, 3 subnets
C      192.168.5.0 is directly connected, FastEthernet0/0.3
C      192.168.5.64 is directly connected, FastEthernet0/0.1
C      192.168.5.128 is directly connected, FastEthernet0/0.2
D   200.1.1.0/24 [90/2172416] via 192.168.5.3, 00:11:30, FastEthernet0/0.3
C   202.2.2.0/24 is directly connected, Serial0/0
S*  0.0.0.0/0 is directly connected, Serial0/0
```

FASE 2: CONFIGURACIÓN DEL ROUTER LINK_2:

TAREAS:

- Enrutamiento EIGRP en el AS 500.
- Modificar la distancia administrativa de la ruta estática hacia la sucursal 2.

DESARROLLO:

1. La configuración muestra que sólo se habilitó el enrutamiento EIGRP en el AS 500, donde sólo se declaran las subredes de la VLAN 10 y 77; la VLAN 20 no lo requiere ya que sólo accederá hacia Internet.
2. Como se requiere de una ruta estática de respaldo entre las sucursales, se modificó la distancia administrativa de la ruta hacia la red 192.168.1.0 /24 a un valor de 180 (mayor que la de EIGRP).
3. Para brindar cierta seguridad en la comunicación se habilita una lista de control de acceso (110), la cual deniega la comunicación de la subred de VLAN 20 hacia la sucursal 2. Se aplica en la entrada de las subinterfaces.

```
LINK_2#SH RUN
!
hostname LINK_2
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.5.66 255.255.255.192
 ip access-group 110 in
!
interface FastEthernet0/0.3
 encapsulation dot1Q 77 native
 ip address 192.168.5.3 255.255.255.192
```

```
 ip access-group 110 in
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.1.1.1 255.255.255.0
 encapsulation frame-relay
 ip summary-address eigrp 500 192.168.5.0 255.255.255.128 5
!
!
router eigrp 500
 network 192.168.5.0 0.0.0.63
 network 192.168.5.64 0.0.0.63
 network 200.1.1.0
 no auto-summary
!
ip classless
ip route 192.168.1.0 255.255.255.0 Serial0/0 180
!
access-list 110 deny ip 192.168.5.128 0.0.0.63 any
!
```

4. Para el caso se necesita modificar el encapsulamiento a Frame Relay, ya que su comunicación hacia el router ALMACÉN pasará por una nube de ese tipo.

```
LINK_2#sh interfaces s0/0
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 200.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation Frame Relay, loopback not set, keepalive set (10 sec)
  LMI enq sent  116, LMI stat recvd 116, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE

……<resultado omitido>……..
```

5. La tabla de enrutamiento en el router muestra que mediante el enrutamiento EIGRP es posible alcanzar las redes 192.168.1.0/24 e Internet; en el caso de Internet, mediante la ruta por defecto redistribuida en el router LINK_1.

```
LINK_2#SH IP ROUTE
……<resultado omitido>……..
Gateway of last resort is 192.168.5.1 to network 0.0.0.0
D    192.168.1.0/24 [90/2172416] via 200.1.1.2, 00:11:58, Serial0/0
     192.168.5.0/26 is subnetted, 2 subnets
C       192.168.5.0 is directly connected, FastEthernet0/0.3
C       192.168.5.64 is directly connected, FastEthernet0/0.1
C    200.1.1.0/24 is directly connected, Serial0/0
D*EX 0.0.0.0/0 [170/2172416] via 192.168.5.1, 00:00:17, FastEthernet0/0.3LINK_2#sh inter
```

FASE 3: CONFIGURACIÓN DE ROUTER ALMACÉN:

TAREAS:

- Enrutamiento EIGRP en el AS 500.
- Modificar la distancia administrativa de las rutas estáticas hacia las VLAN 10 y 77 de la sucursal principal.

DESARROLLO:

1. La configuración muestra que se habilitó el enrutamiento EIGRP en el AS 500.
2. Como se requiere mantener rutas estáticas de respaldo entre las sucursales, se modifico la distancia administrativa de las rutas hacia las redes 192.168.5.0 /26 y 192.168.5.64 /26 a un valor de 180 (mayor que la de EIGRP).

```
ALMACÉN#sh runn
!
hostname ALMACÉN
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 200.1.1.2 255.255.255.0
 encapsulation frame-relay
!
!
router eigrp 500
 network 192.168.1.0
 network 200.1.1.0
 no auto-summary
!
ip classless
ip route 192.168.5.0 255.255.255.192 Serial0/0 180
ip route 192.168.5.64 255.255.255.192 Serial0/0 180
!
```

3. La tabla de enrutamiento en el router muestra que mediante el enrutamiento EIGRP es posible alcanzar las redes 192.168.5.0/26, 192.168.5.64 /26 e Internet; en el caso de Internet, mediante la ruta por defecto redistribuida en el router LINK_1.

```
ALMACÉN#sh ip rout
……<resultado omitido>……..

Gateway of last resort is 200.1.1.1 to network 0.0.0.0
C   192.168.1.0/24 is directly connected, FastEthernet0/0
    192.168.5.0/26 is subnetted, 2 subnets
D      192.168.5.0 [90/2172416] via 200.1.1.1, 00:14:49, Serial0/0
D      192.168.5.64 [90/2172416] via 200.1.1.1, 00:14:49, Serial0/0
C   200.1.1.0/24 is directly connected, Serial0/0
D*EX 0.0.0.0/0 [170/2684416] via 200.1.1.1, 00:03:08, Serial0/0
```

FASE 4: PRUEBAS DE VERIFICACIÓN:

1. Conectividad hacia la red de la sucursal 2 desde el router LINK_1.

```
LINK_1#PING 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/16/19 ms
LINK_1#PING 200.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/14/33 ms
```

2. Conectividad desde un Host de la red principal hacia un servidor de Internet.

```
PC>ping 74.125.45.104
Pinging 74.125.45.104 with 32 bytes of data:
Reply from 74.125.45.104: bytes=32 time=50ms TTL=126
Reply from 74.125.45.104: bytes=32 time=24ms TTL=126
Reply from 74.125.45.104: bytes=32 time=50ms TTL=126
Reply from 74.125.45.104: bytes=32 time=26ms TTL=126
Ping statistics for 74.125.45.104:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 24ms, Maximum = 50ms, Average = 37ms
```

3. Conectividad desde un Host de la red sucursal 2 hacia un servidor de Internet.

```
PC>ping 74.125.45.104
Pinging 74.125.45.104 with 32 bytes of data:
Reply from 74.125.45.104: bytes=32 time=33ms TTL=124
Reply from 74.125.45.104: bytes=32 time=34ms TTL=124
Reply from 74.125.45.104: bytes=32 time=49ms TTL=124
Reply from 74.125.45.104: bytes=32 time=36ms TTL=124
Ping statistics for 74.125.45.104:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 33ms, Maximum = 49ms, Average = 38ms
```

4. Conectividad hacia diversos puntos de la topología desde el router LINK_2.

```
LINK_2#ping 74.125.45.104
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 74.125.45.104, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/39 ms
LINK_2#
LINK_2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/13 ms
LINK_2#ping 200.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
LINK_2#ping 200.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/10 ms
LINK_2#ping 202.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/16/23 ms
LINK_2#ping 202.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/10/22 ms
```

5. Conectividad hacia diversos puntos de la topología.

```
ALMACÉN#ping 74.125.45.104
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 74.125.45.104, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ALMACÉN#ping 74.125.45.104
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 74.125.45.104, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ALMACÉN#ping 200.62.191.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.62.191.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
ALMACÉN#ping
Protocol [ip]:
Target IP address: 74.125.45.104
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: f0/0
% Invalid source
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 74.125.45.104, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/24/28 ms
ALMACÉN#
ALMACÉN#ping 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/22/43 ms
ALMACÉN#ping 192.168.5.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 13/24/45 ms
ALMACÉN#ping 192.168.5.67
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.67, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 17/26/40 ms
```

6. Tabla de traducción NAT, posterior a la prueba de conectividad hacia servidores de Internet y accesos a un servidor web.

```
LINK_1#SH IP NAT TRanslations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.2.2.1:8       192.168.1.2:8      74.125.45.104:8    74.125.45.104:8
icmp 202.2.2.1:2       192.168.5.133:2    200.62.191.11:2    200.62.191.11:2
icmp 202.2.2.1:3       192.168.5.67:3     200.62.191.11:3    200.62.191.11:3
icmp 202.2.2.1:1       192.168.5.68:1     200.62.191.1:1     200.62.191.1:1
icmp 202.2.2.1:1024    192.168.5.68:2     74.125.45.104:2    74.125.45.104:1024
icmp 202.2.2.1:1025    192.168.5.68:3     74.125.45.104:3    74.125.45.104:1025
icmp 202.2.2.1:4       192.168.5.68:4     74.125.45.104:4    74.125.45.104:4
icmp 202.2.2.1:5       192.168.5.68:5     74.125.45.104:5    74.125.45.104:5
icmp 202.2.2.1:6       192.168.5.68:6     74.125.45.104:6    74.125.45.104:6
udp 202.2.2.1:1025     192.168.5.68:1025  200.62.191.11:53   200.62.191.11:53
udp 202.2.2.1:1026     192.168.5.68:1026  200.62.191.11:53   200.62.191.11:53
tcp 202.2.2.1:1025     192.168.5.68:1025  74.125.45.104:80   74.125.45.104:80
```

CONCLUSIONES

_____

_____

_____

_____

TAREAS

- Modifique el encapsulamiento del router LINK_1 hacia Internet con PPP mediante CHAP.
- Habilite un resumen manual en el router LINK_2 para enviarlo por la interfaz serial 0/0.

LABORATORIO N°3 - VLAN CON ENRUTAMIENTO DINÁMICO DE DOS PROTOCOLOS POR CONEXIÓN FRAME RELAY

INTRODUCCIÓN

Las redes Frame Relay presentan una alternativa variada de conexión que puede implementarse con diferentes protocolos de enrutamiento, así como con diferentes servicios.

OBJETIVOS

- Implementación de una conexión Frame Relay mediante dos protocolos de enrutamiento.
- Redistribución de rutas entre protocolos EIGRP y RIP.

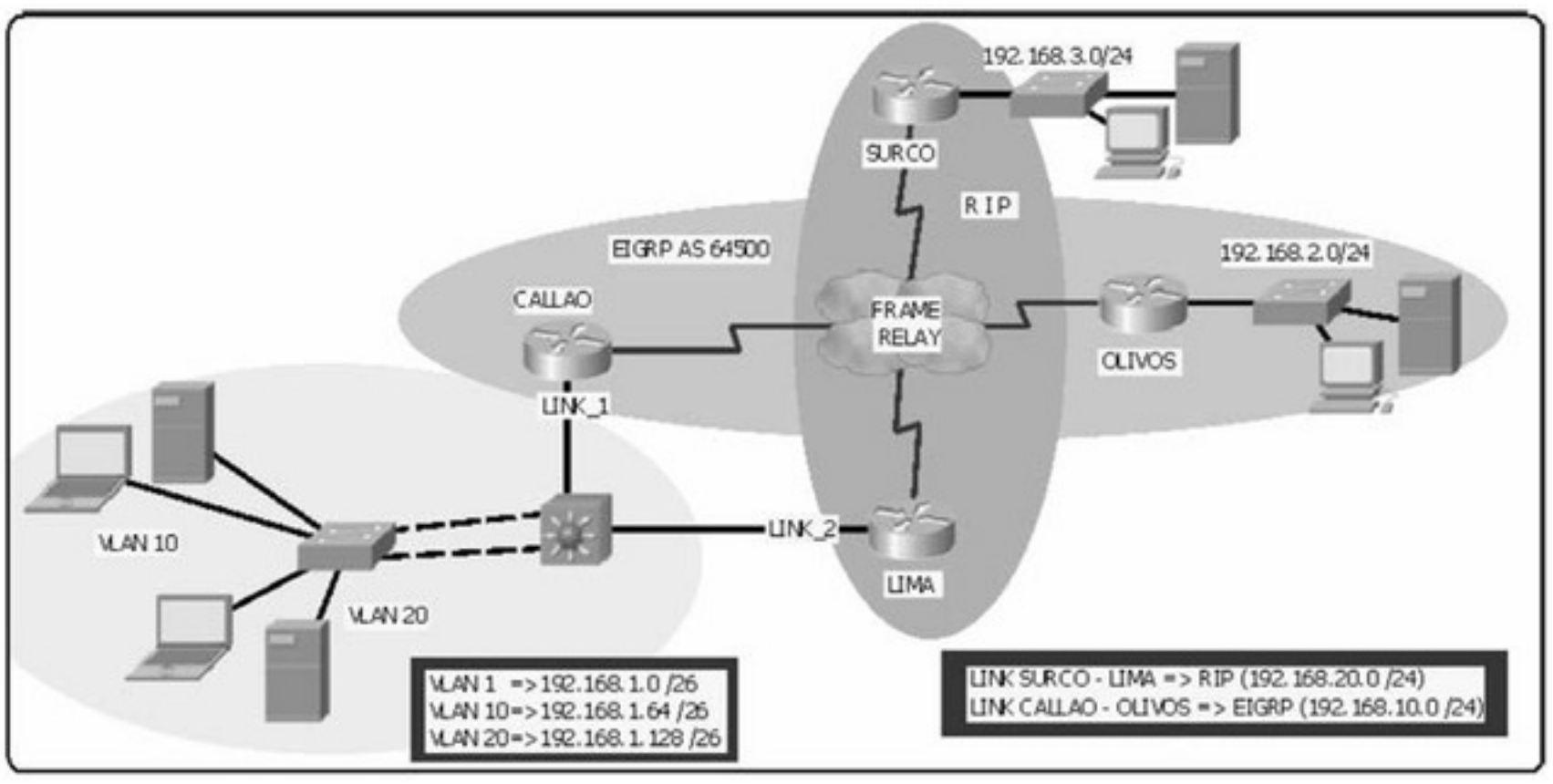
DESCRIPCIÓN

El circuito de red presentado tiene como finalidad permitir a una red de Lan conectarse mediante dos enlaces a otras redes, utilizando los protocolos de enrutamiento RIP y EIGRP, que serán redistribuidos para la comunicación de la topología.

La finalidad del circuito podría ser la comunicación hacia Internet o sucursales de una empresa y los protocolos de enrutamiento pueden ser reemplazados.

El proceso de enrutamiento se realiza mediante una conexión de encapsulamiento Frame Relay en ambas conexiones, donde el switch Frame Relay deberá contar con cuatro DLCI.

La red local emplea VLAN para la segmentación del dominio de broadcast, recibiendo enrutamiento a través de un switch capa 3 que utiliza EIGRP dentro del AS 64500. El switch capa 3 es empleado como recorrido para la comunicación entre el enrutamiento EIGRP y RIP.



FASE I: CONFIGURACIÓN DE RED LOCAL

- Implementación de VLAN.
- Establecer Intervlan.

- Habilitar el protocolo EIGRP.
- Habilitar el servicio DHCP para cada VLAN.

DESARROLLO:

1. El switch capa 3 es configurado para establecer **Intervlan**, definiendo las VLAN y asignando una dirección IP a cada una de las interfaces. Hay que considerar que en el switch capa 3 puede activarse más de una VLAN administrativa.
2. Los puertos de conexión hacia cada router pertenecen a la VLAN 1 administrativa, bajo la cual se pueden comunicar las VLAN 10 y 20 hacia toda la red de la topología.
3. El enrutamiento EIGRP permitirá publicar las subredes de la VLAN hacia los routers Lima y Callao, así como recibir las redes publicadas a través del router Callao y redistribuidas en el router Lima.
4. Completando la configuración en el switch capa 3, se habilita el servicio DHCP para las VLAN 10 y 20.

```
Sw-Layer3#sh run
!
hostname Sw-Layer3
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
……..< resultado omitido >……
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.192
!
interface Vlan10
 ip address 192.168.1.65 255.255.255.192
!
interface Vlan20
 ip address 192.168.1.129 255.255.255.192
!
router eigrp 64500
 network 192.168.1.0 0.0.0.63
 network 192.168.1.64 0.0.0.63
 network 192.168.1.128 0.0.0.63
 no auto-summary
!
ip classless
!
ip dhcp pool VLAN10
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
ip dhcp pool VLAN20
 network 192.168.1.128 255.255.255.192
 default-router 192.168.1.129
!
```

5. La tabla de enrutamiento en el switch capa 3 muestra las redes recibidas por EIGRP (D) y redistribuidas mediante RIP (D EX) en el router Lima.

```
Sw-Layer3#sh ip route
……..< resultado omitido >……

Gateway of last resort is 192.168.1.1 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C      192.168.1.0/26 is directly connected, Vlan1
C      192.168.1.64/26 is directly connected, Vlan10
C      192.168.1.128/26 is directly connected, Vlan20
D    192.168.2.0/24 [90/27772416] via 192.168.1.1, 00:37:43, Vlan1
D EX 192.168.3.0/24 [170/86799872] via 192.168.1.62, 00:32:02, Vlan1
D    192.168.10.0/24 [90/27769856] via 192.168.1.1, 00:37:44, Vlan1
D EX 192.168.20.0/24 [170/86799872] via 192.168.1.62, 00:32:03, Vlan1
```

6. La tabla de vecinos en switch capa 3 indica los vecinos EIGRP que corresponden a los routers Lima y Callao.

```
Sw-Layer3#sh ip eigrp neighbors
IP-EIGRP neighbors for process 64500
H   Address         Interface     Hold Uptime   SRTT   RTO  Q  Seq
                                  (sec)         (ms)       Cnt Num
0   192.168.1.1     Vlan          13  00:39:17  40     1000 0  34
1   192.168.1.62    Vlan          12  00:33:35  40     1000 0  204
```

7. Complementando la configuración de la red Lan, se muestra lo implementado en el switch capa 2.

```
SW-layer2#sh run
!
hostname SW-layer2
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
!
……..< resultado omitido >……
!
interface Vlan1
 ip address 192.168.1.3 255.255.255.192
!
ip default-gateway 192.168.1.62
!
```

FASE II: CONFIGURACIÓN DE CONEXIÓN LINK_1 (LIMA – SURCO)

1. En la configuración del router Lima se centraliza la mayor parte ya que debe trabajar con ambos protocolos en el enrutamiento y redistribuirlos.
2. Nótese que la redistribución se está realizando en cada configuración de enrutamiento, donde se deben indicar las métricas con las que se integran las nuevas redes a cada publicación.
3. Las redes EIGRP, al ser publicadas mediante RIP, ingresarán con una métrica de tres saltos, y las redes RIP ingresarán con un ancho de banda de 256 kbps y un retardo de 20000useg. En realidad, esto estará en función de las características del enlace o un estimado que pueda brindar un promedio de valores.

```
LIMA#sh run
!
hostname LIMA
!
!
interface FastEthernet0/0
 ip address 192.168.1.62 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.254 255.255.255.252
 duplex auto
 speed auto
!
```

```
interface Serial0/0
 ip address 192.168.20.2 255.255.255.0
 encapsulation frame-relay
!
……..< resultado omitido >……
!
router eigrp 64500
 redistribute rip metric 256 20000 255 1 1500
 network 192.168.1.0 0.0.0.63
 no auto-summary
!
router rip
 version 2
 redistribute eigrp 64500 metric 3
 network 192.168.20.0
 no auto-summary
!
```

4. La tabla de enrutamiento en el router Lima muestra cómo se recibe la publicación mediante los dos protocolos.

```
LIMA#sh ip route
……..< resultado omitido >……
Gateway of last resort is not set
    192.168.1.0/26 is subnetted, 3 subnets
C      192.168.1.0 is directly connected, FastEthernet0/0
D      192.168.1.64 [90/25628160] via 192.168.1.2, 00:30:27, FastEthernet0/0
D      192.168.1.128 [90/25628160] via 192.168.1.2, 00:30:27, FastEthernet0/0
D   192.168.2.0/24 [90/2174976] via 192.168.1.1, 00:39:32, FastEthernet0/0
R   192.168.3.0/24 [120/1] via 192.168.20.1, 00:00:09, Serial0/0
D   192.168.10.0/24 [90/2172416] via 192.168.1.1, 00:39:32, FastEthernet0/0
C   192.168.20.0/24 is directly connected, Serial0/0
```

5. La configuración del router Surco no merece mayores comentarios, ya que sólo necesitamos el enrutamiento RIP en versión 2.

```
SURCO#sh run
!
hostname SURCO
!
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
```

6. La tabla de enrutamiento comprueba cómo se reciben las redes redistribuidas mediante el router Lima. Para este caso se indica que tienen una métrica de tres.

```
SURCO#sh ip route
Gateway of last resort is not set
    192.168.1.0/26 is subnetted, 3 subnets
R      192.168.1.0 [120/3] via 192.168.20.2, 00:45:30, Serial0/0
R      192.168.1.64 [120/3] via 192.168.20.2, 00:36:25, Serial0/0
R      192.168.1.128 [120/3] via 192.168.20.2, 00:36:25, Serial0/0
R   192.168.2.0/24 [120/3] via 192.168.20.2, 00:45:30, Serial0/0
C   192.168.3.0/24 is directly connected, FastEthernet0/0
R   192.168.10.0/24 [120/3] via 192.168.20.2, 00:45:30, Serial0/0
C   192.168.20.0/24 is directly connected, Serial0/0
```

FASE III: CONFIGURACIÓN DE LA CONEXIÓN LINK_1 (CALLAO – OLIVOS)

1. El router Callao sólo requiere de la configuración del protocolo EIGRP.

```
CALLAO#sh run
!
hostname CALLAO
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.253 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.10.1 255.255.255.0
 encapsulation frame-relay
!
……..< resultado omitido >……
!
router eigrp 64500
 network 192.168.10.0
 network 192.168.1.0 0.0.0.63
 no auto-summary
!
!
interface Serial0/0
 ip address 192.168.20.1 255.255.255.0
 encapsulation frame-relay
!
……..< resultado omitido >……
!
router rip
 version 2
 network 192.168.3.0
 network 192.168.20.0
 no auto-summary
!
```

2. La tabla de enrutamiento muestra cómo se publican las redes RIP (192.168.3.0 /24 y 192.168.20.0 /24) dentro del enrutamiento EIGRP. Están etiquetadas como D EX, con una distancia administrativa de 170 por defecto y una métrica basada en el ancho de banda con el retardo indicado al redistribuirse.

```
CALLAO#sh ip route
……..< resultado omitido >……
Gateway of last resort is not set
    192.168.1.0/26 is subnetted, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/25628160] via 192.168.1.2, 00:27:22, FastEthernet0/0
D       192.168.1.128 [90/25628160] via 192.168.1.2, 00:27:22, FastEthernet0/0
D    192.168.2.0/24 [90/2172416] via 192.168.10.2, 00:42:07, Serial0/0
D EX 192.168.3.0/24 [170/61202432] via 192.168.1.62, 00:36:25, FastEthernet0/0
C    192.168.10.0/24 is directly connected, Serial0/0
D EX 192.168.20.0/24 [170/61202432] via 192.168.1.62, 00:36:26, FastEthernet0/0
```

3. Los cuatro routers en sus interfaces seriales presentan encapsulamiento mediante Frame Relay.

```
CALLAO#sh interfaces s0/0
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation Frame Relay, loopback not set, keepalive set (10 sec)
  LMI enq sent  534, LMI stat recvd 533, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
……..< resultado omitido >……
```

4. La tabla de enrutamiento indica una información similar a la del router Callao con respecto a las redes redistribuidas (D EX), con una distancia administrativa por defecto de 170 y, en el caso de la métrica, será mayor dado que se suma el retardo del último enlace.

```
OLIVOS#sh ip route
……..< resultado omitido >……

Gateway of last resort is not set
    192.168.1.0/26 is subnetted, 3 subnets
D       192.168.1.0 [90/2172416] via 192.168.10.1, 00:49:27, Serial0/0
D       192.168.1.64 [90/27772416] via 192.168.10.1, 00:34:41, Serial0/0
D       192.168.1.128 [90/27772416] via 192.168.10.1, 00:34:41, Serial0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
D EX 192.168.3.0/24 [170/61714432] via 192.168.10.1, 00:43:45, Serial0/0
C    192.168.10.0/24 is directly connected, Serial0/0
D EX 192.168.20.0/24 [170/61714432] via 192.168.10.1, 00:43:46, Serial0/0
```

5. El router Olivos sólo requiere de la configuración de EIGRP, muy aparte de la configuración básica.

```
OLIVOS#sh running-config
!
hostname OLIVOS
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 192.168.10.2 255.255.255.0
 encapsulation frame-relay
!
……..< resultado omitido >……
!
router eigrp 64500
 network 192.168.10.0
 network 192.168.2.0
 no auto-summary
!
```

FASE IV: TAREAS

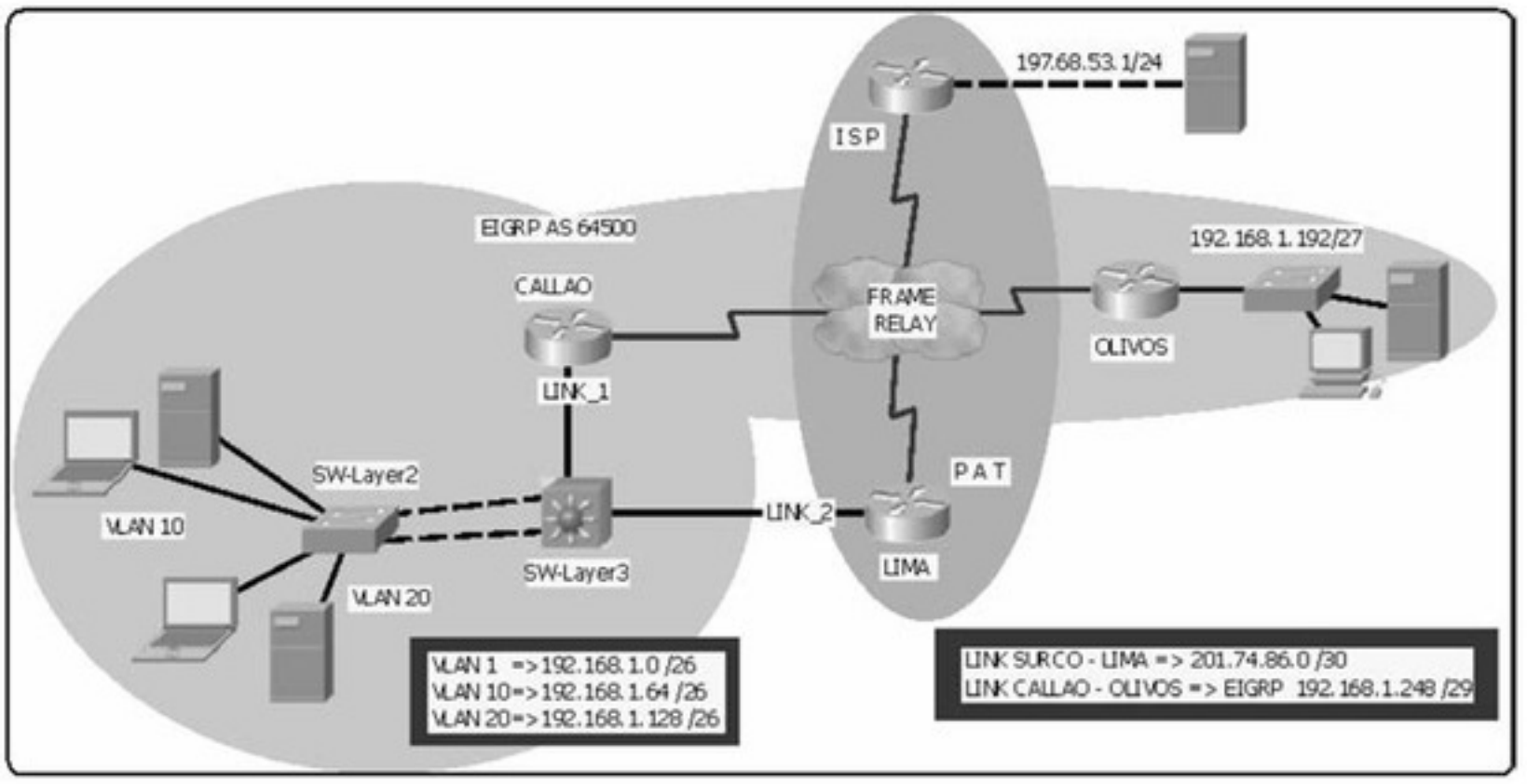
Pueden agregarse algunas configuraciones:

1. Establecer un dominio VTP en la red Lan.
2. Habilitar una autenticación de enrutamiento EIGRP.
3. Crear listas de acceso para que los Hosts de la VLAN10 puedan ingresar sólo a páginas web externas y los de la VLAN20, tanto a páginas WEB como a servicios de correo externos.
4. Modificar el direccionamiento de la red EIGRP a una sola dirección; asimismo, habilitar el servicio PAT en el router Lima (este último caso es desarrollado a continuación).

FASE V: CONFIGURACIÓN DE LA RED CON EIGRP EN EL ENRUTAMIENTO INTERNO Y LA IMPLEMENTACIÓN DE PAT

El esquema de red en este caso es el mismo, lo que se modificó es la configuración del direccionamiento en ciertas redes.

- La red interna maneja la dirección 192.168.1.0 /24 y es ruteada mediante EIGRP en el AS 64500.
- El router Lima utiliza PAT y una ruta por defecto que redistribuye en EIGRP.
- El router ISP no maneja el enrutamiento hacia la red interna.
- El switch capa 3 mantiene su configuración anterior.
- Los routers Callao y Olivos sólo necesitan modificar su información de enrutamiento.



1. La configuración del router Lima presenta la mayor parte del trabajo para el cumplimiento de todo el proceso de comunicación.
2. Obsérvese que se configuró una **access list 20** que se integra con la sentencia para el servicio PAT, indicando que las direcciones del rango 192.168.1.0 /24 serán traducidas a la dirección de la interfaz serial pero con un puerto diferente.

```
LIMA#sh run
!
hostname LIMA
!
!
interface FastEthernet0/0
 ip address 192.168.1.62 255.255.255.192
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 201.74.86.2 255.255.255.252
 encapsulation frame-relay
```

```
 ip nat outside
!
……..< resultado omitido >……
!
router eigrp 64500
 redistribute static
 network 192.168.1.0 0.0.0.63
 no auto-summary
!
ip nat inside source list 20 interface Serial0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!
access-list 20 permit 192.168.1.0 0.0.0.255
!
```

3. Las tablas de enrutamiento en los routers Olivos, Callao y sw-layer3, muestran las redes EIGRP publicadas, así como la ruta por defecto redistribuida por el router Lima.

```
LIMA#sh ip route
Gateway of last resort is 201.74.86.1 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks
C      192.168.1.0/26 is directly connected, FastEthernet0/0
D      192.168.1.64/26 [90/25628160] via 192.168.1.2, 02:33:36, FastEthernet0/0
D      192.168.1.128/26 [90/25628160] via 192.168.1.2, 02:33:36, FastEthernet0/0
D      192.168.1.192/27 [90/2174976] via 192.168.1.1, 01:24:00, FastEthernet0/0
D      192.168.1.248/29 [90/2172416] via 192.168.1.1, 01:24:00, FastEthernet0/0
    201.74.86.0/30 is subnetted, 1 subnets
C      201.74.86.0 is directly connected, Serial0 /0
S*   0.0.0.0/0 [1/0] via 201.74.86.1
           is directly connected, Serial0/0
```

```
OLIVOS#sh ip route
Gateway of last resort is 192.168.1.253 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks
D      192.168.1.0/26 [90/2172416] via 192.168.1.253, 01:26:16, Serial0/0
D      192.168.1.64/26 [90/27772416] via 192.168.1.253, 01:26:16, Serial0/0
D      192.168.1.128/26 [90/27772416] via 192.168.1.253, 01:26:16, Serial0/0
C      192.168.1.192/27 is directly connected, FastEthernet0/0
C      192.168.1.248/29 is directly connected, Serial0/0
D*EX 0.0.0.0/0 [170/7292416] via 192.168.1.253, 01:26:16, Serial0/0
```

```
CALLAO#sh ip route
Gateway of last resort is 192.168.1.62 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks
C      192.168.1.0/26 is directly connected, FastEthernet0/0
D      192.168.1.64/26 [90/25628160] via 192.168.1.2, 02:36:59, FastEthernet0/0
D      192.168.1.128/26 [90/25628160] via 192.168.1.2, 02:36:59, FastEthernet0/0
D      192.168.1.192/27 [90/2172416] via 192.168.1.254, 01:27:23, Serial0/0
C      192.168.1.248/29 is directly connected, Serial0/0
D*EX 0.0.0.0/0 [170/6780416] via 192.168.1.62, 01:37:15, FastEthernet0/0
```

```
Sw-Layer3#sh ip route
Gateway of last resort is 192.168.1.62 to network 0.0.0.0
    192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks
C       192.168.1.0/26 is directly connected, Vlan1
C       192.168.1.64/26 is directly connected, Vlan10
C       192.168.1.128/26 is directly connected, Vlan20
D       192.168.1.192/27 [90/27772416] via 192.168.1.1, 00:00:02, Vlan1
D       192.168.1.248/29 [90/27769856] via 192.168.1.1, 00:00:02, Vlan1
D*EX 0.0.0.0/0 [170/32377856] via 192.168.1.62, 00:00:02, Vlan1
```

4. El router ISP no necesita habilitar enrutamiento, por lo que muestra las redes directamente conectadas.

```
ISP#sh ip route
Gateway of last resort is not set
C    197.68.53.0/24 is directly connected, FastEthernet0/0
     201.74.86.0/30 is subnetted, 1 subnets
C       201.74.86.0 is directly connected, Serial0/0
```

5. El servicio NAT de sobrecarga (PAT) indica a través de su tabla la traducción de direcciones que emplea la dirección IP (201.74.86.2) de la interfaz serial 0/0 con diferente puerto, cada vez que un Host de la red 192.168.1.0 /24 quiere alcanzar la red externa.

```
LIMA#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 201.74.86.2:10    192.168.1.1:10     197.68.53.1:10     197.68.53.1:10
icmp 201.74.86.2:11    192.168.1.1:11     197.68.53.1:11     197.68.53.1:11
icmp 201.74.86.2:5     192.168.1.194:5    197.68.53.1:5      197.68.53.1:5
icmp 201.74.86.2:6     192.168.1.194:6    197.68.53.1:6      197.68.53.1:6
icmp 201.74.86.2:4     192.168.1.254:4    197.68.53.1:4      197.68.53.1:4
icmp 201.74.86.2:1024  192.168.1.254:5    197.68.53.254:5    197.68.53.254:1024
icmp 201.74.86.2:1025  192.168.1.254:6    197.68.53.254:6    197.68.53.254:1025
icmp 201.74.86.2:7     192.168.1.254:7    197.68.53.254:7    197.68.53.254:7
```

FASE VI: CONCLUSIONES:

LABORATORIO N° 4 - REDISTRIBUCIÓN DE RUTAS

INTRODUCCIÓN

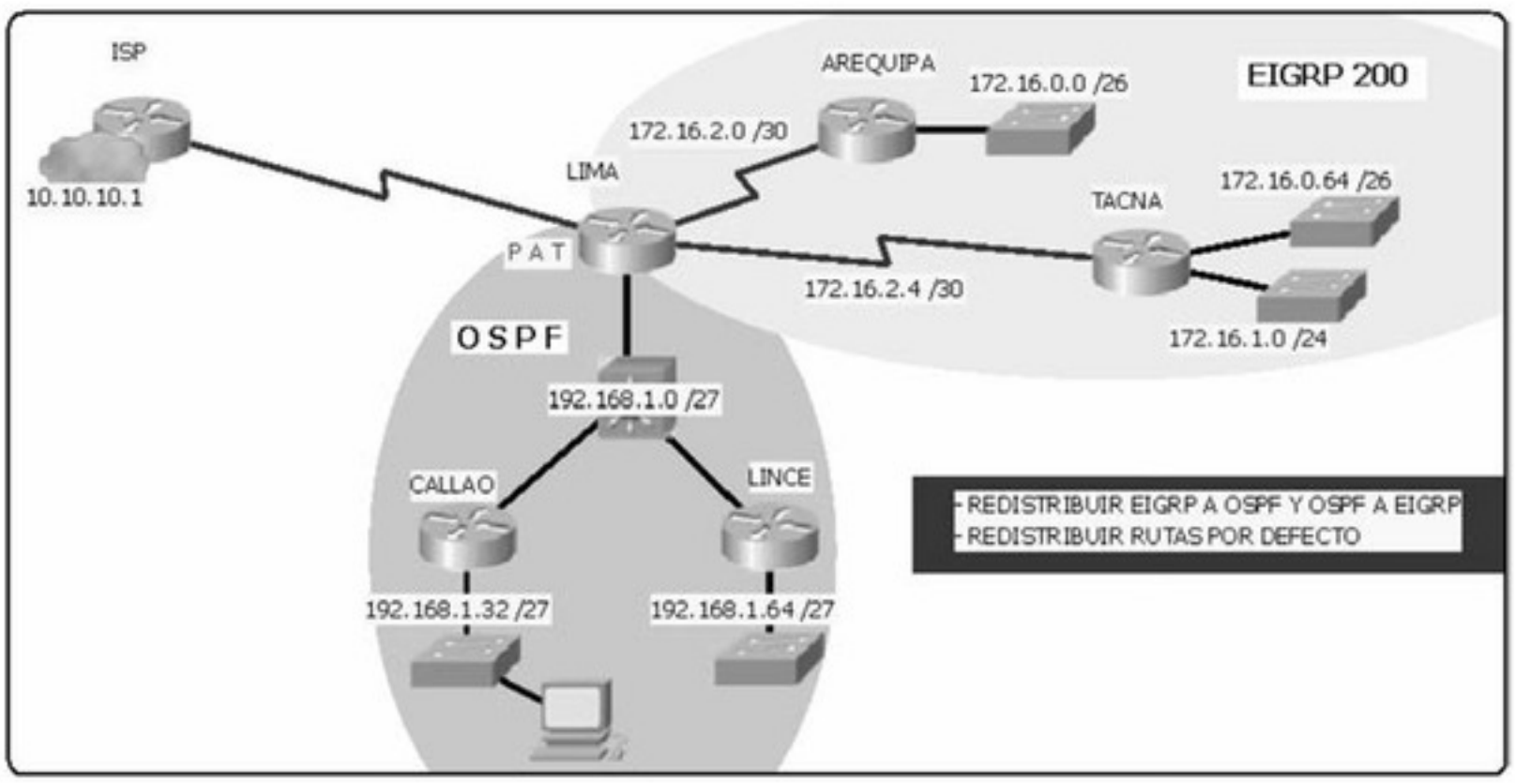
Es común en redes internas y externas el uso de protocolos de enrutamiento junto a rutas por defecto o rutas estáticas, por lo cual se aplican redistribuciones sencillas para que dichas redes sean propagadas dentro del enrutamiento dinámico; pero, asimismo, pueden redistribuirse protocolos de enrutamiento distintos, tipo EIGRP y OSPF, donde se deberá considerar la métrica de cada uno de ellos y se deberán emplear los términos más adecuados para facilitar la identificación de cada una de la rutas.

OBJETIVO

- Configuración del enrutamiento OSPF y EIGRP con la redistribución para ambos casos.

DESCRIPCIÓN

La topología exige el manejo de dos protocolos de enrutamiento (OSPF y EIGRP); asimismo, cada uno de los routers del esquema deberá tener alcance hacia Internet. Para la red de OSPF se exige que el router Lince sea configurado como DR y el router Callao, como BDR, mientras que el router Lima no participará de la elección.



DESARROLLO

El router Lima es un router de borde, router frontera o router de salida, al ubicarse en ese punto, por lo que será el encargado de realizar el proceso de redistribución para las rutas estáticas OSPF y EIGRP.

Considerando los laboratorios iniciales, se van a obviar algunas partes de la configuración asumiendo su entendimiento y desarrollo.

- Realice las rutinas de diagnóstico y deje listos los equipos para su configuración.
- Realice la conexión física de los equipos en base a la topología de red.
- Habilite la opción de captura de texto en el emulador (Hyperterminal).

1. Configuración de enrutamiento
   - Luego de la configuración básica, habilitaremos los enrutamientos EIGRP y OSPF, respectivamente, en cada equipo.
   - Los routers del área 0, en OSPF, presentan una interfaz loopback, la cual permitirá definir el ID de cada router. Se debe tener en cuenta que para el caso del router Lima debe configurarse lo siguiente:

```
router eigrp 200
network 172.16.2.0 0.0.0.3
 network 172.16.2.4 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
network 192.168.1.0 0.0.0.31 area 0
```

2. Verificación de la configuración
   - Verificamos en cada router el protocolo habilitado con ayuda del comando "**show ip protocol**".

```
LIMA#sh ip protocols
Routing Protocol is "eigrp  200 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 200
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.2.0/30
    172.16.2.4/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.2.2      90            18950
    172.16.2.5      90            19387
  Distance: internal 90 external 170
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 203.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.31 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.3         110       00:11:40
    192.168.1.2         110       00:11:38
  Distance: (default is 110)
```

- Realizamos el diagnóstico de vecinos OSPF, donde se comprueba que se han identificado todos los vecinos, con el inconveniente de que el router Lince no ha sido elegido como DR, sino el router Callao.

```
LIMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
207.7.7.7         1   FULL/BDR          00:00:33    192.168.1.3     FastEthernet0/0
205.5.5.5         1   FULL/DR         00:00:33    192.168.1.2     FastEthernet0/0
```

```
LINCE#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
205.5.5.5         1   FULL/DR         00:00:33    192.168.1.2     FastEthernet0/0
203.3.3.3         1   FULL/DROTHER    00:00:38    192.168.1.1     FastEthernet0/0
```

```
CALLAO#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
207.7.7.7         1   FULL/BDR          00:00:30    192.168.1.3     FastEthernet0/0
203.3.3.3         1   FULL/DROTHER    00:00:35    192.168.1.1     FastEthernet0/0
```

- Realizamos el diagnóstico de vecinos EIGRP, donde se identifica a los vecinos en base al IP de conexión.

```
LIMA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0   172.16.2.2      Se0/0           13  00:12:03  40     1000 0  40
1   172.16.2.5      Se0/2           14  00:12:03  40     1000 0  28
```

```
TACNA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0   172.16.2.6      Se0/0           12  00:18:00  40     1000 0  17
```

```
AREQUIPA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0   172.16.2.1      Se0/0           12  00:17:13  40     1000 0  17
```

3. DR y BDR
   - Habilitamos la configuración de prioridad para las interfaces FastEthernet 0/0 en cada router OSPF, dando mayor prioridad al router Lince y colocando en 0 la prioridad del router Lima, ya que no participará:

```
Interface fastehernet 0/0
ip ospf priority 255
```

- Se reinicia el proceso OSPF en cada router.

```
Clear ip OSPF  process 1
```

- Realizamos el diagnóstico de vecinos OSPF nuevamente y comprobamos que el router Lince es elegido como DR y el router Callao, como BDR.

```
LIMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
207.7.7.7       255   FULL/DR         00:00:33    192.168.1.3     FastEthernet0/0
205.5.5.5       200   FULL/BDR        00:00:33    192.168.1.2     FastEthernet0/0
```

```
LINCE#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
205.5.5.5       200   FULL/BDR        00:00:33    192.168.1.2     FastEthernet0/0
203.3.3.3       0   FULL/DROTHER      00:00:38    192.168.1.1     FastEthernet0/0
```

```
CALLAO#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
207.7.7.7       255   FULL/DR         00:00:30    192.168.1.3     FastEthernet0/0
203.3.3.3       0   FULL/DROTHER      00:00:35    192.168.1.1     FastEthernet0/0
```

- Realizamos el diagnóstico de las interfaces mediante OSPF, indicándose la prioridad asignada anteriormente, así como el ID del router, el intervalo de intercambio Hello, entre otras opciones.

```
LIMA# sh ip ospf interface f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/27, Area 0
  Process ID 1, Router ID 203.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 207.7.7.7, Interface address 192.168.1.3
  Backup Designated Router (ID) 205.5.5.5, Interface address 192.168.1.2
  ……..<resultado omitido>……..
```

```
CALLAO#sh ip ospf interface f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.2/27, Area 0
  Process ID 1, Router ID 205.5.5.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 200
  Designated Router (ID) 207.7.7.7, Interface address 192.168.1.3
  Backup Designated Router (ID) 205.5.5.5, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
……..<resultado omitido>……..
```

```
LINCE# sh ip ospf interface f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.3/27, Area 0
  Process ID 1, Router ID 207.7.7.7, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 207.7.7.7, Interface address 192.168.1.3
  Backup Designated Router (ID) 205.5.5.5, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
……..<resultado omitido>……..
```

4. TABLA DE ENRUTAMIENTO 1:

- Se muestran las redes, tanto de OSPF en los routers Lima, Callao y Lince, como de EIGRP en los routers Lima, Tacna y Arequipa, faltando las rutas externas de cada protocolo.
- Obsérvese que todas las rutas están visualizadas en el router Lima, por lo que faltará redistribuirlas y completar la configuración.

```
LIMA#sh ip route
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D       172.16.0.0/26 [90/2172416] via 172.16.2.2, 00:11:42, Serial0/0
D       172.16.0.64/26 [90/2172416] via 172.16.2.5, 00:11:42, Serial0/2
D       172.16.1.0/24 [90/2172416] via 172.16.2.5, 00:11:42, Serial0/2
C       172.16.2.0/30 is directly connected, Serial0/0
C       172.16.2.4/30 is directly connected, Serial0/2
     192.168.1.0/27 is subnetted, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
O       192.168.1.32 [110/2] via 192.168.1.2, 00:11:06, FastEthernet0/0
O       192.168.1.64 [110/2] via 192.168.1.3, 00:11:06, FastEthernet0/0
     200.1.1.0/30 is subnetted, 1 subnets
C       200.1.1.0 is directly connected, Serial0/1
C    203.3.3.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Serial0/1
```

```
CALLAO#sh ip route ospf
     192.168.1.0/27 is subnetted, 3 subnets
O       192.168.1.64 [110/2] via 192.168.1.3, 00:22:31, FastEthernet0/0
```

```
LINCE#sh ip route ospf
     192.168.1.0/27 is subnetted, 3 subnets
O       192.168.1.32 [110/2] via 192.168.1.2, 00:23:40, FastEthernet0/0
```

```
AREQUIPA#sh ip route eigrp
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D       172.16.0.64/26 [90/2684416] via 172.16.2.1, 00:17:07, Serial0/0
D       172.16.1.0/24 [90/2684416] via 172.16.2.1, 00:17:07, Serial0/0
D       172.16.2.4/30 [90/2681856] via 172.16.2.1, 00:17:07, Serial0/0
```

```
TACNA#sh ip route eigrp
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D       172.16.0.0/26 [90/2684416] via 172.16.2.6, 00:17:52, Serial0/0
D       172.16.2.0/30 [90/2681856] via 172.16.2.6, 00:17:52, Serial0/0
```

5. REDISTRIBUCIÓN:

1. El router Lima presenta una ruta por defecto hacia el ISP, el cual deberá ser redistribuido hacia las redes OSPF y EIGRP.

```
router eigrp 200
redistribute static
!
router ospf 1
default-information originate
```

2. Luego se habilita la redistribución, en el router Lima, de OSPF a EIGRP y viceversa, de la siguiente manera. Para este procedimiento deberán considerarse las métricas con las que cuenta cada protocolo.

```
router eigrp 200
 redistribute ospf 1 metric 64 1 255 1 1500
!
router ospf 1
redistribute eigrp 200
```

6. TABLA DE ENRUTAMIENTO II:

1. Una vez completado el proceso de redistribución se puede conocer toda la topología y realizar las pruebas respectivas de acceso, conectividad, entre otras.

```
LIMA#sh ip route
……<resultado omitido>……..
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D      172.16.0.0/26 [90/2172416] via 172.16.2.2, 00:11:42, Serial0/0
D      172.16.0.64/26 [90/2172416] via 172.16.2.5, 00:11:42, Serial0/2
D      172.16.1.0/24 [90/2172416] via 172.16.2.5, 00:11:42, Serial0/2
C      172.16.2.0/30 is directly connected, Serial0/0
C      172.16.2.4/30 is directly connected, Serial0/2
    192.168.1.0/27 is subnetted, 3 subnets
C      192.168.1.0 is directly connected, FastEthernet0/0
O      192.168.1.32 [110/2] via 192.168.1.2, 00:11:06, FastEthernet0/0
O      192.168.1.64 [110/2] via 192.168.1.3, 00:11:06, FastEthernet0/0
    200.1.1.0/30 is subnetted, 1 subnets
C      200.1.1.0 is directly connected, Serial0/1
C    203.3.3.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Serial0/1
```

2. Los routers Lince y Callao observarán las redes EIGRP y la ruta por defecto, con una etiqueta **O E2**.

```
CALLAO#sh ip route
……<resultado omitido>……..
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
O E2 172.16.0.0/16 [110/20] via 192.168.1.1, 00:14:52, FastEthernet0/0
    192.168.1.0/27 is subnetted, 3 subnets
C      192.168.1.0 is directly connected, FastEthernet0/0
C      192.168.1.32 is directly connected, FastEthernet0/1
O      192.168.1.64 [110/2] via 192.168.1.3, 00:22:31, FastEthernet0/0
    205.5.5.0/32 is subnetted, 1 subnets
C      205.5.5.5 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 00:14:52, FastEthernet0/0
```

```
LINCE#sh ip route
……<resultado omitido>……..
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
O E2 172.16.0.0/16 [110/20] via 192.168.1.1, 00:15:51, FastEthernet0/0
    192.168.1.0/27 is subnetted, 3 subnets
C      192.168.1.0 is directly connected, FastEthernet0/0
O      192.168.1.32 [110/2] via 192.168.1.2, 00:23:40, FastEthernet0/0
C      192.168.1.64 is directly connected, FastEthernet0/1
    207.7.7.0/32 is subnetted, 1 subnets
C      207.7.7.7 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 00:15:51, FastEthernet0/0
```

3. Los routers Arequipa y Tacna mostrarán las rutas OSPF con una etiqueta **D EX**, así como la ruta por defecto.

```
AREQUIPA#sh ip route
……..<resultado omitido>……..
Gateway of last resort is 172.16.2.1 to network 0.0.0.0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C       172.16.0.0/26 is directly connected, FastEthernet0/0
D       172.16.0.64/26 [90/2684416] via 172.16.2.1, 00:17:07, Serial0/0
D       172.16.1.0/24 [90/2684416] via 172.16.2.1, 00:17:07, Serial0/0
C       172.16.2.0/30 is directly connected, Serial0/0
D       172.16.2.4/30 [90/2681856] via 172.16.2.1, 00:17:07, Serial0/0
    192.168.1.0/27 is subnetted, 3 subnets
D EX    192.168.1.0 [170/40512256] via 172.16.2.1, 00:17:08, Serial0/0
D EX    192.168.1.32 [170/40512256] via 172.16.2.1, 00:16:31, Serial0/0
D EX    192.168.1.64 [170/40512256] via 172.16.2.1, 00:16:31, Serial0/0
D*EX 0.0.0.0/0 [170/7289856] via 172.16.2.1, 00:17:08, Serial0/0
```

```
TACNA#sh ip route
……..<resultado omitido>……..
Gateway of last resort is 172.16.2.6 to network 0.0.0.0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D       172.16.0.0/26 [90/2684416] via 172.16.2.6, 00:17:52, Serial0/0
C       172.16.0.64/26 is directly connected, FastEthernet0/0
C       172.16.1.0/24 is directly connected, FastEthernet0/1
D       172.16.2.0/30 [90/2681856] via 172.16.2.6, 00:17:52, Serial0/0
C       172.16.2.4/30 is directly connected, Serial0/0
    192.168.1.0/27 is subnetted, 3 subnets
D EX    192.168.1.0 [170/40512256] via 172.16.2.6, 00:17:52, Serial0/0
D EX    192.168.1.32 [170/40512256] via 172.16.2.6, 00:17:16, Serial0/0
D EX    192.168.1.64 [170/40512256] via 172.16.2.6, 00:17:16, Serial0/0
D*EX 0.0.0.0/0 [170/7289856] via 172.16.2.6, 00:17:52, Serial0/0
```

4. El router ISP no requiere de enrutamiento alguno para comunicarse con la red interna pues las direcciones son traducidas a la dirección 200.1.1.1.

```
ISP#sh ip route
……..<resultado omitido>……..
Gateway of last resort is not set
    10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Loopback0
    200.1.1.0/30 is subnetted, 1 subnets
C       200.1.1.0 is directly connected, Serial0/0
```

7. Configuración de PAT

   - Se necesita configurar una lista de control de acceso para facilitar el servicio NAT; asimismo, la sentencia de NAT relaciona la lista de acceso 30 para que los Hosts que contiene sean traducidos a la dirección de la interfaz serial 0/1, con diferente número de puerto.

```
ip nat inside source list 30 interface Serial0/1 overload
!
access-list 30 permit 192.168.1.0 0.0.0.255
access-list 30 permit 172.16.0.0 0.0.3.255
interface FastEthernet0/0
ip nat inside
```

```
!
interface Serial0/0
ip nat inside
!
interface Serial0/1
ip nat outside
!
interface Serial0/2
ip nat inside
```

8. Tabla NAT

Se indica la traducción de direcciones que realiza el router, empleando la dirección de la interfaz serial 0/1 (200.1.1.1):

```
LIMA#sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.1:1026    172.16.2.2:1       200.1.1.2:1        200.1.1.2:1026
icmp 200.1.1.1:1024    172.16.2.5:1       200.1.1.2:1        200.1.1.2:1024
icmp 200.1.1.1:1025    192.168.1.2:1      200.1.1.2:1        200.1.1.2:1025
icmp 200.1.1.1:1       192.168.1.3:1      200.1.1.2:1        200.1.1.2:1
icmp 200.1.1.1:1027    192.168.1.34:1     200.1.1.2:1        200.1.1.2:1027
```

9. Identificación de redistribución en el router Lima.

```
LIMA#sh ip protocols
Routing Protocol is "eigrp  200 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 200, ospf 1 , static
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.2.0/30
    172.16.2.4/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.2.2      90            18950
    172.16.2.5      90            19387
  Distance: internal 90 external 170
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 203.3.3.3
Redistributing External Routes from,
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.31 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.3         110       00:11:40
    192.168.1.2         110       00:11:38
  Distance: (default is 110)
```

1. Configuración final.
    - Router Lima

```
LIMA#sh run
!
!
!
interface Loopback0
 ip address 203.3.3.3 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
 ip ospf priority 255
 ip nat inside
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 172.16.2.1 255.255.255.252
 ip nat inside
 clock rate 64000
!
interface Serial0/1
 ip address 200.1.1.1 255.255.255.252
 ip nat outside
!
interface Serial0/2
 ip address 172.16.2.6 255.255.255.252
 ip nat inside
 clock rate 64000
!
router eigrp 200
 redistribute ospf 1 metric 64 1 255 1 1500
 redistribute static
 network 172.16.2.0 0.0.0.3
 network 172.16.2.4 0.0.0.3
 no auto-summary
!
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 200
 network 192.168.1.0 0.0.0.31 area 0
 default-information originate
!
ip nat inside source list 30 interface Serial0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1
!
!
access-list 30 permit 192.168.1.0 0.0.0.255
access-list 30 permit 172.16.0.0 0.0.3.255
!
```

- Router Callao

```
CALLAO#sh run
!
!
!
interface Loopback0
 ip address 205.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.224
 ip ospf priority 200
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.33 255.255.255.224
 duplex auto
 speed auto
!
……<resultado omitido>……
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.1.32 0.0.0.31 area 0
!
```

- Router Lince

```
LINCE#sh run
!
!
interface Loopback0
 ip address 207.7.7.7 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.3 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.65 255.255.255.224
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.1.64 0.0.0.31 area 0
!
```

- Router Arequipa

```
AREQUIPA#sh run
!
hostname AREQUIPA
!
!
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.255.192
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 172.16.2.2 255.255.255.252
!
……..<resultado omitido>……..
!
router eigrp 200
 network 172.16.0.0
 no auto-summary
!
```

- Router Tacna

```
TACNA#sh runn
!
hostname TACNA
!
!
interface FastEthernet0/0
 ip address 172.16.0.65 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
!
router eigrp 200
 network 172.16.0.0
 no auto-summary
!
```

- Router ISP

```
ISP#sh run
!
hostname ISP
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.0
!
!
interface Serial0/0
 ip address 200.1.1.2 255.255.255.252
 clock rate 64000
!
……<resultado omitido>……
!
ip classless
ip route 192.168.1.0 255.255.255.0 Serial0/0
ip route 172.16.0.0 255.255.0.0 Serial0/0
!
```

CONCLUSIONES

_____

_____

_____

_____

TAREAS

- Modifique el encapsulamiento de los routers hacia Internet con PPP, mediante CHAP.
- Habilite una autenticación en el enrutamiento OSPF y EIGRP.

LABORATORIO N° 5 - SWITCHING y ROUTING

INTRODUCCIÓN

Switching IP de nivel 3 OSI es equivalente al enrutado TCP/IP. Normalmente los routers se encuentran en esta capa. El protocolo ARP es el que se utiliza para asignar direcciones IP a direcciones MAC. La función router es incluida en el hardware de los switches. De esta forma se consigue una enorme mejora en el rendimiento, comparando un switch que opera a nivel 3 y esta misma función realizada por un router normal. Un switch de nivel 3 puede trabajar a más de 10 veces la velocidad de un router tradicional.

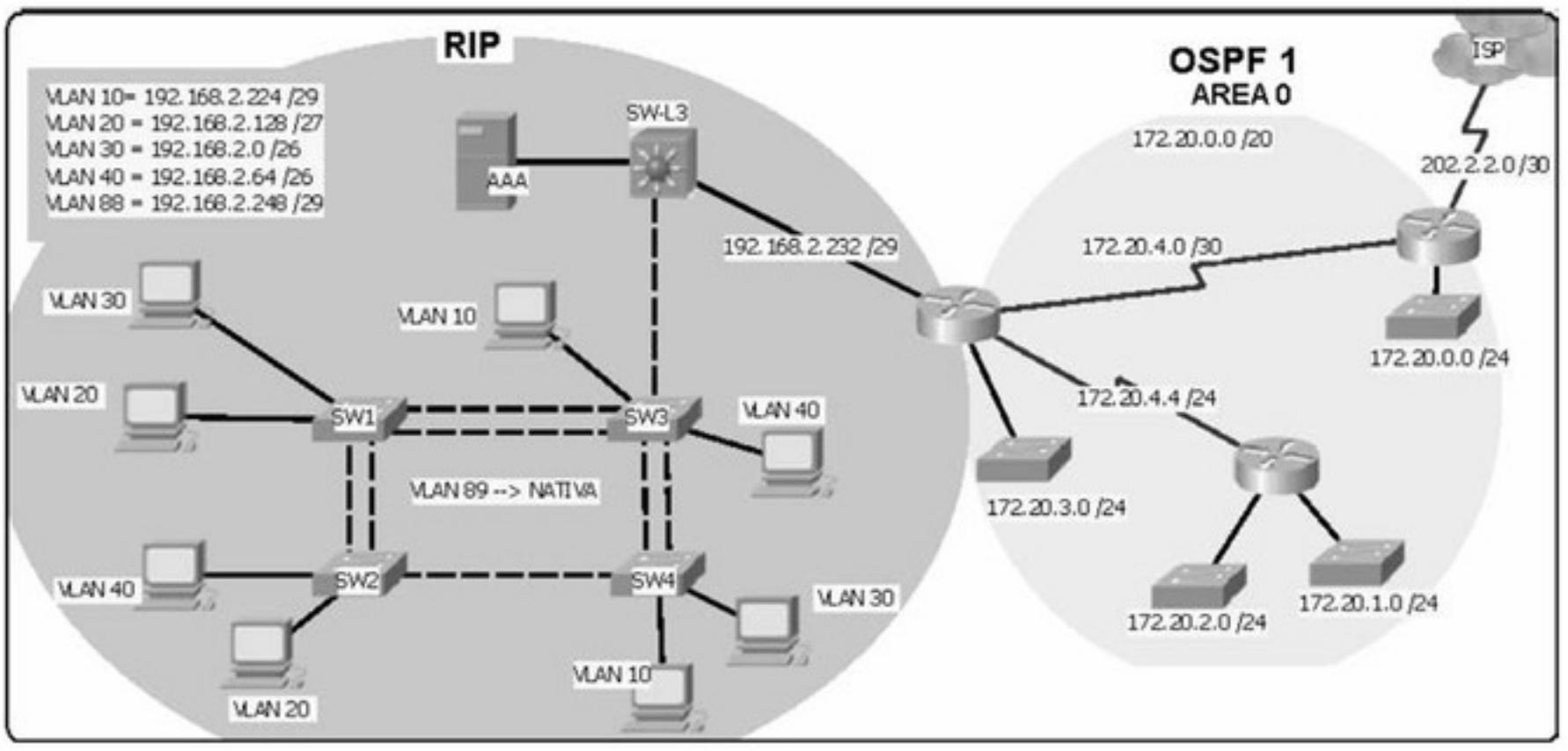
Este tipo de switches integra routing y switching para producir altas velocidades (medidas en millones de paquetes por segundo). Estos dispositivos son el resultado de un proceso de evolución natural de las redes de área local, ya que combinan las funciones de los switches capa 2 con la capacidad de los routers.

OBJETIVOS

- Configuración de enrutamiento y redistribución de rutas entre RIP y OSPF.
- Configuración de un switch capa 3.
- Habilitar una autenticación mediante un servidor Radius.

DESCRIPCIÓN

El siguiente esquema representa una conexión entre un proveedor de servicios y una empresa, donde se emplea un enrutamiento mediante OSPF al área de backbone, que posteriormente incorporará otras áreas. Asimismo, existe una oficina sucursal (red Campus) que se enlaza con el área 0 de OSPF mediante una conexión Ethernet, donde se emplean VLAN administrados en un dominio VTP.



REQUERIMIENTOS:

- Establecer un dominio VTP con las siguientes características:

Dominio : cisco2
password: class
SW-L3 - Server
SW1 - Server
SW3 - Transparente
SW2 - Cliente1
SW4 - Cliente2

- Establezca que el Root para spanning tree sea el switch SW-L3 para todas las VLAN, definiéndose por su valor de prioridad.
- Habilite un servidor de autenticación Radius.
- Configure las VLAN de acuerdo al esquema, donde sólo deberán existir Hosts para las VLAN que se observan en cada switch. Asimismo, defina como VLAN nativa y administrativa a la VLAN 89.
- Habilite la autenticación en un servidor Radius cuando se necesite acceder vía Telnet hacia el switch SW-L3 y el router Norte.
- El switch SW-L3 deberá asignar IP hacia todas la VLAN del dominio VTP, excepto las Vlan administrativas.
- Realice el proceso de redistribución en el router Norte para el enrutamiento RIP y OSPF.
- La conexión entre el router Norte y el switch SW-L3 deberá pertenecer a una subred y se asignará una dirección IP al switch.

DESARROLLO

FASE 1: CONFIGURACIÓN DE CONMUTACIÓN

- Para la configuración básica podemos tomar como referencia los laboratorios del capítulo de Swithcing, así como para la configuración inicial de Vlan y del dominio VTP.
- Para mantener la redundancia en la topología conmutada se ha agregado una conexión entre el switch SW-L3 (Fa0/4) y el switch SW-1 (Fa0/24).

1. Configuración de VLAN
   - Se configura cada uno de los switches para establecer la configuración del dominio VTP, donde los switches SW-L3 y SW-4 son servidores, los switches SW-1 y SW-2 son clientes y el switch SW-3 es transparente.
   - En el switch SW-L3 se configuran las Vlan 10, 20, 30, 40 y 89; asimismo, se crean las interfaces para cada una y se asigna una dirección IP. Hay que considerar que un switch de capa 3 permite activar más de una interfaz VLAN.
   - Al tener más de una interfaz VLAN activa, el switch SW-L3 trabajará como puerta de enlace para cada una.

```
interface Vlan10
 ip address 192.168.2.225 255.255.255.248
interface Vlan20
 ip address 192.168.2.129 255.255.255.224
interface Vlan30
 ip address 192.168.2.1 255.255.255.192
interface Vlan40
 ip address 192.168.2.65 255.255.255.192
interface Vlan89
 ip address 192.168.2.249 255.255.255.248
```

2. En los switch capa 2 se define la Vlan 89 como Vlan nativa, con las siguientes direcciones:

```
SWITCH 1
interface Vlan89
 ip address 192.168.2.254 255.255.255.248
!
SWITCH 2
interface Vlan89
 ip address 192.168.2.252 255.255.255.248
!
SWITCH 3
interface Vlan89
 ip address 192.168.2.253 255.255.255.248
!
SWITCH 4
 interface Vlan89
 ip address 192.168.2.254 255.255.255.248
```

3. Spanning tree
   - Se define la prioridad spanning tree para que el switch SW-L3 sea elegido como root en todas las Vlan.

```
spanning-tree vlan 10,20,30,40,89 priority 4096
```

4. Autenticación
   - Se deberá habilitar el proceso de autenticación en el cual se define un perfil denominado "**telnet_lines**".
   - El servidor Radios tiene la dirección 192.168.2.250 con la clave "**vlan001**".
   - Finalmente se integra dentro del acceso al terminal virtual.

```
aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
!
radius-server host 192.168.2.250 auth-port 1645 key vlan001
line vty 0 15
login authent telnet_lines
```

5. DHCP en SW-L3
   - Se define la configuración siguiente para asignarse a cada Vlan; asimismo, se definen las direcciones a excluir.

```
ip dhcp pool vlan10
network 192.168.2.224 255.255.255.248
default-route 192.168.2.225
ip dhcp pool vlan20
network 192.168.2.128 255.255.255.224
default-route 192.168.2.129
ip dhcp pool vlan30
network 192.168.2.0 255.255.255.192
default-route 192.168.2.1
ip dhcp pool vlan40
network 192.168.2.64 255.255.255.192
default-route 192.168.2.249
!
ip dhcp exclu 192.168.2.225 192.168.2.229
ip dhcp exclu 192.168.2.129 192.168.2.133
ip dhcp exclu 192.168.2.1 192.168.2.5
ip dhcp exclu 192.168.2.65 192.168.2.69
```

FASE 2: DIAGNÓSTICO DE CONFIGURACIÓN EN LOS SWITCHES

1. Dominio VTP
   - En el SW-2 y SW-4 se verifica el modo cliente, con un número de revisión 6, actualizado desde el Host 192.168.2.254.

```
SW-2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD5 0x09 0xB1 0xFF 0x80 0x2D 0x90 0xC9
Configuration last modified by 192.168.2.254 at 3-1-93 01:08:35
```

```
SW-4#SH VTP STAtus
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD5 0x09 0xB1 0xFF 0x80 0x2D 0x90 0xC9
Configuration last modified by 192.168.2.254 at 3-1-93 01:08:35
```

- Se observa que nadie actualiza el switch SW-3 ya que está en modo transparente y su numero de revisión está en 0.

```
SW-3#  sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xB3 0x31 0xD9 0xC8 0xDC 0x83 0xDE
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

- En el switch SW-1 y SW-L3 se observa que la última configuración desde 192.168.2.254 es el modo servidor, en el dominio VTP.

```
SW-1#  sh vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD5 0x09 0xB1 0xFF 0x80 0x2D 0x90 0xC9
Configuration last modified by 192.168.2.254 at 3-1-93 01:08:35
Local updater ID is 192.168.2.254 on interface Vl89 (lowest numbered VLAN interface found)
```

2. VLAN

- Se observa que los switches SW-1 (modo Server) y SW-3 (modo transparente) presentan las Vlan definidas para el domino VTP.

```
SW-1#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   VLAN0010                          active
20   VLAN0020                          active    Fa0/5
30   VLAN0030                          active    Fa0/6
40   VLAN0040                          active
89   VLAN0089                          active
----------< resultado omitido>.....
```

```
SW-3# sh vlan brief
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                            Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                            Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                            Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                            Fa0/23
10   VLAN0010                       active    Fa0/5
20   VLAN0020                       active
30   VLAN0030                       active
40   VLAN0040                       active    Fa0/6
89   VLAN0089                       active
-----------< resultado omitido>.....
```

FASE III: DIAGNÓSTICO DE FUNCIONAMIENTO EN LOS SWITCHES

1. DEFINICIÓN DEL ROOT SPANNING TREE

   - El diagnóstico spanning tree indica que para todas las Vlan el switch SW-L3 es el root, con una prioridad de 4096.
   - La prioridad configurada en el switch es 4096, sin embargo, en cada Vlan se le suma el valor de número.

```
SW-L3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4106  (priority 4096 sys-id-ext 10)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4116  (priority 4096 sys-id-ext 20)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    4126
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4126  (priority 4096 sys-id-ext 30)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    4136
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4136  (priority 4096 sys-id-ext 40)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0089
  Spanning tree enabled protocol ieee
  Root ID    Priority    4185
             Address     0010.1197.2B67
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4185  (priority 4096 sys-id-ext 89)
             Address     0010.1197.2B67
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

- En el switch SW-3 se comprueba la operación spanning tree, con la diferencia de que todos los switches capa 2 tienen entre tres y cuatro enlaces troncales. De similares características es la información que se mostraría en el switch SW-1.

```
SW-3# sh spanning-tree
VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    32769
         Address     0001.C726.7BEA
         Cost        19
         Port        1(FastEthernet0/1)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Desg FWD 19        128.24   P2p

VLAN0010
 Spanning tree enabled protocol ieee
 Root ID    Priority    4106
         Address     0010.1197.2B67
         Cost        19
         Port        24(FastEthernet0/24)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/24           Root FWD 19        128.24   P2p

VLAN0020
 Spanning tree enabled protocol ieee
 Root ID    Priority    4116
         Address     0010.1197.2B67
         Cost        19
         Port        24(FastEthernet0/24)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
         Address     00D0.BA52.951D
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Root FWD 19        128.24   P2p
```

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    4126
             Address     0010.1197.2B67
             Cost        19
             Port        24(FastEthernet0/24)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     00D0.BA52.951D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Root FWD 19        128.24   P2p

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID    Priority    4136
             Address     0010.1197.2B67
             Cost        19
             Port        24(FastEthernet0/24)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32808  (priority 32768 sys-id-ext 40)
             Address     00D0.BA52.951D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/24           Root FWD 19        128.24   P2p

VLAN0089
  Spanning tree enabled protocol ieee
  Root ID    Priority    4185
             Address     0010.1197.2B67
             Cost        19
             Port        24(FastEthernet0/24)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32857  (priority 32768 sys-id-ext 89)
             Address     00D0.BA52.951D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Root FWD 19        128.24   P2p
```

FASE IV: CONFIGURACIÓN DEL ROUTER:

El circuito de red está dividido en dos áreas, una que corresponde al enrutamiento RIP donde interviene el router Norte y el switch SW-L3. La siguiente área es de enrutamiento OSPF, donde también deberá configurarse el router Norte junto con los routers Sur y Borde.

1. ENRUTAMIENTO RIP

- En el switch SW-L3 se habilita de la siguiente manera el enrutamiento y, a su vez, se deshabilitan las actualizaciones por ciertas interfaces.

```
router rip
 version 2
passive-interface default
 no passive-interface FastEthernet0/1
 network 192.168.2.0
 no auto-summary
```

- En el router Norte no debe considerarse la red 172.20.0.0, ya que se definirá dentro del enrutamiento OSPF.

```
router rip
 version 2
  passive-interface default
 no passive-interface FastEthernet0/0
network 192.168.2.0
 no auto-summary
```

2. ENRUTAMIENTO OSPF Y RUTA POR DEFECTO

- Todos los routers del área tendrán una dirección loopback que será empleada como **ID del router**, por lo que deberá ser configurada antes del enrutamiento.

```
ROUTER SUR#
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
router ospf 1
network 172.20.4.4 0.0.0.3 area 0
 network 172.20.2.0 0.0.0.255 area 0
 network 172.20.1.0 0.0.0.255 area 0
```

- En el router Norte, al configurar el enrutamiento OSPF no deberá declararse la red 192.168.2.0.

```
ROUTER NORTE#
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
router ospf 1
 network 172.20.4.0 0.0.0.3 area 0
 network 172.20.4.4 0.0.0.3 area 0
 network 172.20.3.0 0.0.0.255 area 0
!
```

- El router Borde tendrá una ruta por defecto.

```
ROUTER BORDE#
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
router ospf 1
network 172.20.0.0 0.0.0.255 area 0
 network 172.20.4.0 0.0.0.3 area 0

!
ip route 0.0.0.0 0.0.0.0 202.2.2.2
```

3. REDISTRIBUCIÓN:

   Este proceso es como una traducción de direcciones, donde se declaran las redes de acuerdo con la métrica de cada protocolo de enrutamiento.

```
ROUTER NORTE#
router ospf 1
redistribute rip subnets
!
router rip
redistribute ospf 1 metric 4
```

- Para la redistribución de la ruta por defecto en OSPF, se requiere de lo siguiente:

```
ROUTER BORDE#
router ospf 1
default-information originate
```

4. AUTENTICACIÓN
   a. La configuración es similar al switch SW-L3.
   b. Se deberá habilitar el proceso de autenticación en el cual se define un perfil denominado "**telnet_lines**".
   c. El servidor Radios tiene la dirección 192.168.2.250 con la clave "**vlan001**".
   d. Finalmente se integra dentro del acceso al terminal virtual.

```
aaa new-model
!
aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
!
radius-server host 192.168.2.250 auth-port 1645 key vlan001
!
line vty 0 4
login authentication telnet_lines
```

DIAGNÓSTICO DE ENRUTAMIENTO

1. PROTOCOLOS HABILITADOS

```
NORTE#sh ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 15 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip, ospf 1
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0    2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     192.168.2.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
     172.20.4.1           120      01:12:32
     172.20.4.6           120      01:12:32
     0.0.0.0            120      01:12:47
     172.20.3.0           120      01:12:42
     192.168.2.233        120      00:00:14
Distance: (default is 120)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
Redistributing External Routes from,
    rip
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.20.4.0 0.0.0.3 area 0
    172.20.4.4 0.0.0.3 area 0
    172.20.3.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.20.4.1           110      00:11:15
    172.20.4.6           110      00:11:15
  Distance: (default is 110)
```

2. TABLA DE VECINOS

- Se indica la vecindad entre los routers Borde, Norte y Sur.

```
NORTE#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:38    172.20.4.1      Serial0/0
2.2.2.2           0   FULL/  -        00:00:30    172.20.4.6      Serial0/1
```

```
SUR#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    172.20.4.5      Serial0/0
```

```
BORDE#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    172.20.4.2      Serial0/0
```

3. BASE DE DATOS TOPOLÓGICA

- Desde el switch SW-L3 se muestran todas las redes a ser alcanzadas.

```
SW-L3#sh ip rip database
0.0.0.0/0
    [4] via 192.168.2.234, 01:16:07, FastEthernet0/1
172.20.0.0/24
    [4] via 192.168.2.234, 01:16:07, FastEthernet0/1
172.20.1.0/24
    [4] via 192.168.2.234, 01:16:07, FastEthernet0/1
172.20.2.0/24
    [4] via 192.168.2.234, 01:16:07, FastEthernet0/1
172.20.3.0/24
    [4] via 192.168.2.234, 00:00:03, FastEthernet0/1
172.20.4.0/30
    [4] via 192.168.2.234, 01:16:22, FastEthernet0/1
172.20.4.4/30
    [4] via 192.168.2.234, 01:16:22, FastEthernet0/1
192.168.2.0/26    directly connected, Vlan30
192.168.2.64/26   directly connected, Vlan40
192.168.2.128/27  directly connected, Vlan20
192.168.2.224/29  directly connected, Vlan10
192.168.2.232/29  directly connected, FastEthernet0/1
192.168.2.248/29  directly connected, Vlan89
```

4. TABLAS DE ENRUTAMIENTO

- Se indican las mejores rutas hacia cada destino. Obsérvese que aparecen redes con el código O E2, ya que se trata de redes externas, redistribuidas hacia OSPF.

```
SUR#sh ip route
Gateway of last resort is 172.20.4.5 to network 0.0.0.0
     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
     172.20.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.20.0.0/24 [110/129] via 172.20.4.5, 01:13:57, Serial0/0
C       172.20.1.0/24 is directly connected, FastEthernet0/1
C       172.20.2.0/24 is directly connected, FastEthernet0/0
O       172.20.3.0/24 [110/65] via 172.20.4.5, 01:13:57, Serial0/0
O       172.20.4.0/30 [110/128] via 172.20.4.5, 01:13:57, Serial0/0
C       172.20.4.4/30 is directly connected, Serial0/0
     192.168.2.0/24 is variably subnetted, 5 subnets, 4 masks
O E2    192.168.2.0/24 [110/20] via 172.20.4.5, 01:13:57, Serial0/0
O E2    192.168.2.64/26 [110/20] via 172.20.4.5, 01:13:57, Serial0/0
O E2    192.168.2.128/27 [110/20] via 172.20.4.5, 01:13:57, Serial0/0
O E2    192.168.2.224/29 [110/20] via 172.20.4.5, 01:13:57, Serial0/0
O E2    192.168.2.248/29 [110/20] via 172.20.4.5, 01:13:57, Serial0/0
O*E2 0.0.0.0/0 [110/1] via 172.20.4.5, 01:13:57, Serial0/0
```

```
NORTE#sh ip route
Gateway of last resort is 172.20.4.1 to network 0.0.0.0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback0
     172.20.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.20.0.0/24 [110/65] via 172.20.4.1, 00:02:22, Serial0/0
O       172.20.1.0/24 [110/65] via 172.20.4.1, 00:02:22, Serial0/0
O       172.20.2.0/24 [110/65] via 172.20.4.6, 00:02:22, Serial0/1
C       172.20.3.0/24 is directly connected, FastEthernet0/1
C       172.20.4.0/30 is directly connected, Serial0/0
C       172.20.4.4/30 is directly connected, Serial0/1
     192.168.2.0/24 is variably subnetted, 6 subnets, 4 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/0
R       192.168.2.0/26 [120/1] via 192.168.2.233, 00:00:15, FastEthernet0/0
R       192.168.2.64/26 [120/1] via 192.168.2.233, 00:00:15, FastEthernet0/0
R       192.168.2.128/27 [120/1] via 192.168.2.233, 00:00:15, FastEthernet0/0
R       192.168.2.224/29 [120/1] via 192.168.2.233, 00:00:15, FastEthernet0/0
R       192.168.2.248/29 [120/1] via 192.168.2.233, 00:00:15, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 172.20.4.1, 00:02:22, Serial0/0
```

```
BORDE#sh ip route
Gateway of last resort is 202.2.2.2 to network 0.0.0.0
     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     172.20.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.20.0.0/24 is directly connected, FastEthernet0/0
O       172.20.1.0/24 [110/129] via 172.20.4.2, 01:14:50, Serial0/0
O       172.20.2.0/24 [110/129] via 172.20.4.2, 01:14:50, Serial0/0
O       172.20.3.0/24 [110/65] via 172.20.4.2, 01:14:50, Serial0/0
C       172.20.4.0/30 is directly connected, Serial0/0
O       172.20.4.4/30 [110/128] via 172.20.4.2, 01:14:50, Serial0/0
     192.168.2.0/24 is variably subnetted, 5 subnets, 4 masks
O E2    192.168.2.0/24 [110/20] via 172.20.4.2, 01:14:50, Serial0/0
O E2    192.168.2.64/26 [110/20] via 172.20.4.2, 01:14:50, Serial0/0
O E2    192.168.2.128/27 [110/20] via 172.20.4.2, 01:14:50, Serial0/0
O E2    192.168.2.224/29 [110/20] via 172.20.4.2, 01:14:50, Serial0/0
O E2    192.168.2.248/29 [110/20] via 172.20.4.2, 01:14:50, Serial0/0
     202.2.2.0/30 is subnetted, 1 subnets
C       202.2.2.0 is directly connected, Serial0/1
S*   0.0.0.0/0 [1/0] via 202.2.2.2
```

- Se muestran las redes RIP, redistribuidas en el router Norte.

```
SW-L3#sh ip route
Gateway of last resort is 192.168.2.234 to network 0.0.0.0
     172.20.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.20.0.0/24 [120/4] via 192.168.2.234, 01:16:16, FastEthernet0/1
R       172.20.1.0/24 [120/4] via 192.168.2.234, 01:16:16, FastEthernet0/1
R       172.20.2.0/24 [120/4] via 192.168.2.234, 01:16:16, FastEthernet0/1
R       172.20.3.0/24 [120/4] via 192.168.2.234, 00:00:12, FastEthernet0/1
R       172.20.4.0/30 [120/4] via 192.168.2.234, 01:16:31, FastEthernet0/1
R       172.20.4.4/30 [120/4] via 192.168.2.234, 01:16:31, FastEthernet0/1
     192.168.2.0/24 is variably subnetted, 6 subnets, 3 masks
C       192.168.2.0/26 is directly connected, Vlan30
```

```
C     192.168.2.64/26 is directly connected, Vlan40
C     192.168.2.128/27 is directly connected, Vlan20
C     192.168.2.224/29 is directly connected, Vlan10
C     192.168.2.232/29 is directly connected, FastEthernet0/1
C     192.168.2.248/29 is directly connected, Vlan89
R*   0.0.0.0/0 [120/4] via 192.168.2.234, 01:16:16, FastEthernet0/1
```

- El ISP utiliza rutas estáticas, una para cada red.

```
ISP#SH IP ROUTE
Gateway of last resort is not set
    172.20.0.0/20 is subnetted, 1 subnets
S      172.20.0.0 [1/0] via 202.2.2.2
S   192.168.2.0/24 [1/0] via 202.2.2.2
    202.2.2.0/30 is subnetted, 1 subnets
C      202.2.2.0 is directly connected, Serial0/0
ISP#
```

5. CONFIGURACIÓN FINAL

   a. Se presenta la configuración final de los equipos donde se concentra el mayor trabajo, como son: el switch SW_L3 y el router Norte.

```
SW-L3#sh run
Building configuration...
Current configuration : 2771 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW-L3
!
!
!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
!
aaa new-model
!
aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
!
!
!
!
spanning-tree vlan 10,20,30,40,89 priority 4096
!
!
!
interface FastEthernet0/1
 no switchport
 ip address 192.168.2.233 255.255.255.248
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 89
 switchport mode access
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.2.225 255.255.255.248
!
interface Vlan20
 ip address 192.168.2.129 255.255.255.224
!
interface Vlan30
 ip address 192.168.2.1 255.255.255.192
!
interface Vlan40
 ip address 192.168.2.65 255.255.255.192
!
interface Vlan89
 ip address 192.168.2.249 255.255.255.248
!
router rip
 version 2
passive-interface default
 no passive-interface FastEthernet0/1
 network 192.168.2.0
 no auto-summary
!
!
!
ip dhcp excluded-address 192.168.2.225 192.168.2.229
ip dhcp excluded-address 192.168.2.129 192.168.2.133
ip dhcp excluded-address 192.168.2.1 192.168.2.5
ip dhcp excluded-address 192.168.2.65 192.168.2.69
!
ip dhcp pool vlan10
 network 192.168.2.224 255.255.255.248
 default-router 192.168.2.225
ip dhcp pool vlan20
 network 192.168.2.128 255.255.255.224
 default-router 192.168.2.129
```

```
ip dhcp pool vlan30
 network 192.168.2.0 255.255.255.192
 default-router 192.168.2.1
ip dhcp pool vlan40
 network 192.168.2.64 255.255.255.192
 default-router 192.168.2.249
!
!
radius-server host 192.168.2.250 auth-port 1645 key vlan001
!!
!
line con 0
 login
line vty 0 4
 login
 login authentication telnet_lines
line vty 5 15
 login
 login authentication telnet_lines
!
!
End
```

```
NORTE#sh run
Building configuration...
Current configuration : 1517 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname NORTE
!
!!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
!
aaa new-model
!
aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
!
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.2.234 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 172.20.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.20.4.2 255.255.255.252
 clock rate 64000
!
interface Serial0/1
 ip address 172.20.4.5 255.255.255.252
 clock rate 64000
!
!
router ospf 1
 log-adjacency-changes
 redistribute rip subnets
 network 172.20.4.0 0.0.0.3 area 0
 network 172.20.4.4 0.0.0.3 area 0
 network 172.20.3.0 0.0.0.255 area 0
!
router rip
 version 2
 redistribute ospf 1 metric 4
 network 192.168.2.0
 no auto-summary
!
ip classless
!
!
!
!
!
radius-server host 192.168.2.250 auth-port 1645 key vlan001
!
!
!
line con 0
 login
line vty 0 4
 login
 login authentication telnet_lines
line vty 5 15
 login
 login authentication telnet_lines
!
!
!
end
```

- Configuración en los switches de capa 2.

```
SW-1#SH RUN
!
!
interface FastEthernet0/1
switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 20
!
interface FastEthernet0/6
 switchport access vlan 30
!
!
!
interface FastEthernet0/24
switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan89
 ip address 192.168.2.254 255.255.255.248
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

```
SW-3#sh run
!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
vtp domain cisco2
vtp mode transparent
vtp password class
vtp version 2
!
!
vlan 10
vlan 20
vlan 30
vlan 40
vlan 89
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 10
!
interface FastEthernet0/6
 switchport access vlan 40
!
!
!
interface FastEthernet0/24
switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
switchport trunk native vlan 89
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan89
 ip address 192.168.2.253 255.255.255.248
!
```

```
SW-2#SH RUNN
!
!
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 40
!
interface FastEthernet0/6
 switchport access vlan 20
!
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan89
 ip address 192.168.2.252 255.255.255.248
!
!
```

```
SW-4# sh run
!
!
interface FastEthernet0/1
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 89
```

```
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 89
 switchport trunk allowed vlan 10,20,30,40,89
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
 switchport access vlan 10
!
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan89
 ip address 192.168.2.251 255.255.255.248
!
!
```

- Configuración de los routers Sur, Norte e ISP.

```
SUR#sh runn
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.20.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.20.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.20.4.6 255.255.255.252
!
!
router ospf 1
 log-adjacency-changes
 network 172.20.4.4 0.0.0.3 area 0
 network 172.20.2.0 0.0.0.255 area 0
 network 172.20.1.0 0.0.0.255 area 0
!
!
!
```

```
ISP#SH RUN
!
!
interface Serial0/0
 ip address 202.2.2.1 255.255.255.252
!
!
ip classless
ip route 172.20.0.0 255.255.240.0 202.2.2.2
ip route 192.168.2.0 255.255.255.0 202.2.2.2
!
!
```

```
BORDE#sh run
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.20.4.1 255.255.255.252
!
interface Serial0/1
 ip address 202.2.2.1 255.255.255.252
 clock rate 64000
!
!
router ospf 1
 log-adjacency-changes
 network 172.20.0.0 0.0.0.255 area 0
 network 172.20.4.0 0.0.0.3 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 202.2.2.2
!
!
```

OBSERVACIONES Y/O COMENTARIOS

_____

_____

_____

_____

TAREAS

- Habilite PAT en el router de borde.
- Modifique el protocolo de enrutamiento a OSPF o EIGRP.
- Habilite la seguridad de puerto en su switch.

LABORATORIO N° 6 - LISTAS DE CONTROL DE ACCESO

DESCRIPCIÓN

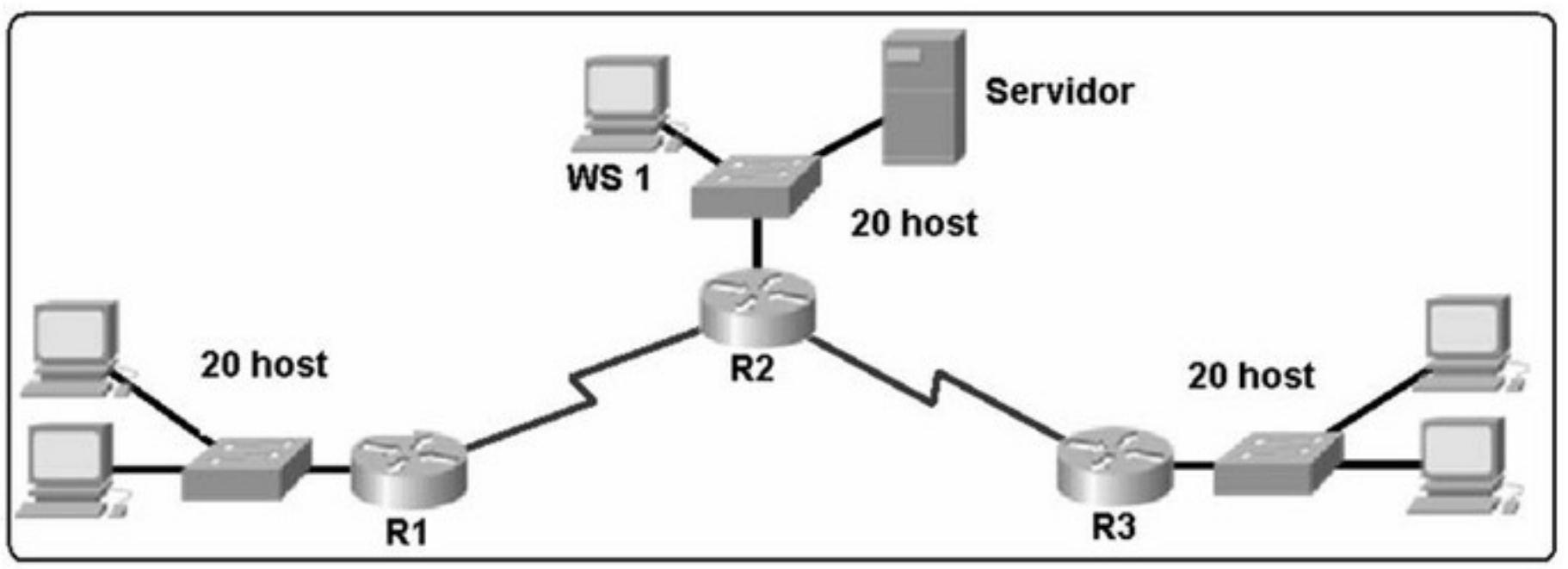
Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar el tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

OBJETIVOS

- Realizar la implementación básica y avanzada de la configuración EIGRP.
- Aplicar adecuadamente las listas de control de acceso de acuerdo a ciertos requerimientos de conexión.

DESCRIPCIÓN

El presente proyecto consistirá en diseñar y poner en marcha una red implementada para una empresa con sedes en tres lugares diferentes, para lo cual se estudió, estableció y probó el diseño de la red y subredes a implementarse.



Los requerimientos solicitados son los siguientes:

Fase 1: Para el direccionamiento IP deberá definirse una dirección de acuerdo al número de Hosts requeridos.

Fase 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

Fase 3: Para esta etapa, la red y subredes establecidas deberán tener una interconexión total, quiere decir que todos los terminales (Hosts) de todas las subredes deberán “verse” y comunicarse unos a otros sin restricción alguna.

Fase 4: Implementar la seguridad en la red, debido a que algunos Hosts de cierta parte de la red no deben tener acceso a otra parte de dicha red, vale decir, se debe restringir el acceso y comunicación entre Hosts de acuerdo a los requerimientos solicitados por el administrador de red.

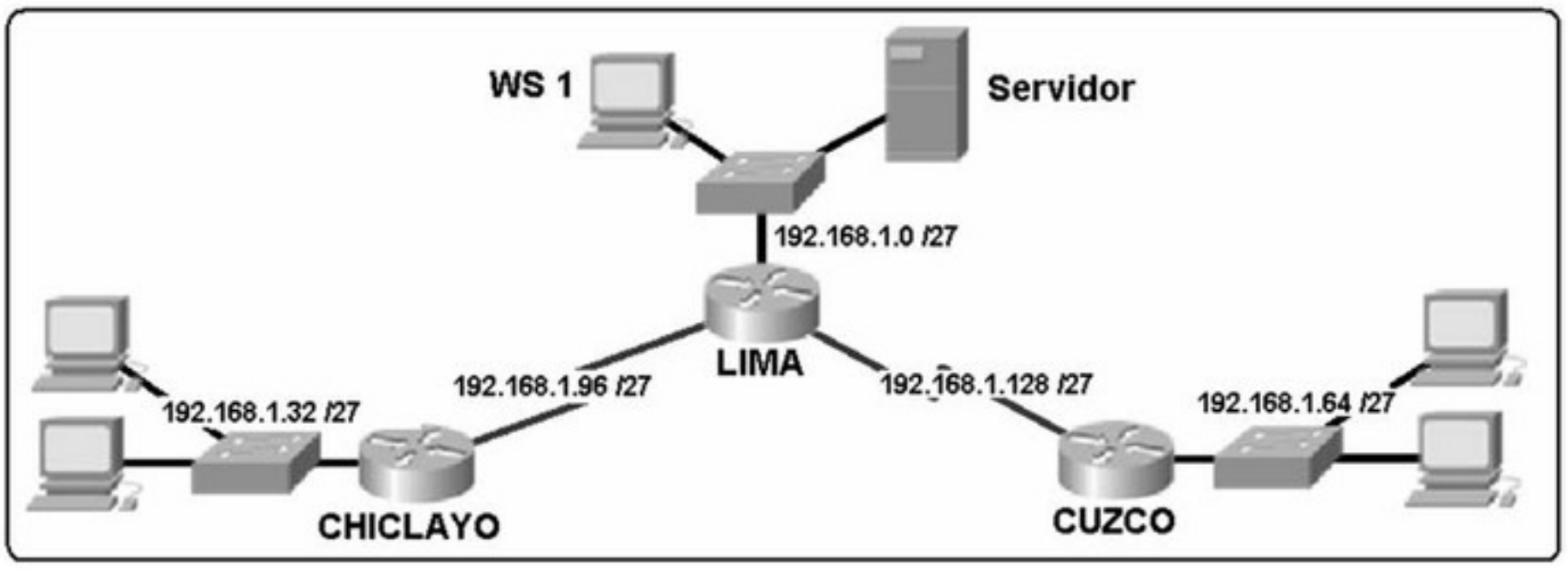
Fase 5: Comprobación total de los dispositivos instalados, así como del funcionamiento satisfactorio de la red implementada de acuerdo a las especificaciones solicitadas.

Fase 6: Configuración final.

DESARROLLO

FASE 1.- ASIGNACIÓN DE DIRECCIONES DE IP:

1. Para cumplir satisfactoriamente los requerimientos solicitados en esta fase, dividiremos la red (subneteo) realizando una segmentación en ocho partes, ya que más adelante la empresa puede crecer y se necesitarían mas subredes, teniendo en cuenta que la cantidad de Hosts de cada subred es por el momento pequeña.
2. Asignaremos a nuestra red el IP: 192.168.1.0



FASE 2.-CONFIGURACIÓN BÁSICA:

1. En la siguiente planilla estableceremos la configuración básica de los routers, teniendo en cuenta las subredes obtenidas anteriormente, y así poder hacer un seguimiento del proceso de configuración.

	R1	R2	R3
Nombre de Host	CHICLAYO	LIMA	CUZCO
Dirección de IP en Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de IP en Serial 0/1	……	192.168.1.130	……
Dirección de IP en Fa 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	eigrp	eigrp	eigrp
Sistema autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

2. Diagnóstico de vecinos Cisco:

```
LIMA#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0         121          S      2950        Fas 0/1
CUZCO        Ser 0/1         121          R      C2600       Ser 0/0
CHICLAYO     Ser 0/0         121          R      C2600       Ser 0/0
```

```
CUZCO#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0         154          S      2950        Fas 0/1
LIMA         Ser 0/0         154          R      C2600       Ser 0/1
```

```
CHICLAYO#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0         169          S      2950        Fas 0/1
LIMA         Ser 0/0         169          R      C2600       Ser 0/0
```

3. Prueba de conectividad:

```
LIMA#PING 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/12 ms

LIMA#PING 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/33 ms
```

FASE 3.-CONFIGURACIÓN DE ENRUTAMIENTO:

1. Asignación del protocolo de ruteo

```
router eigrp 200
 network 192.168.1.0 0.0.0.31
 network 192.168.1.96 0.0.0.31
 network 192.168.1.128 0.0.0.31
 no auto-summary
```

2. Tabla de vecinos:

   - Verificamos si existe vecindad con los routers configurados bajo EIGRP.

```
CHICLAYO#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                              (sec)       (ms)      Cnt Num
0  192.168.1.98  Ser0/0        11  00:10:54 40    1000 0  11
```

```
LIMA#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                              (sec)       (ms)      Cnt Num
0  192.168.1.131 Ser0/1        14  00:13:33 40    1000 0  12
1  192.168.1.99  Ser0/0        11  00:13:20 40    1000 0  7
```

```
CUZCO#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H  Address       Interface    Hold Uptime   SRTT  RTO  Q  Seq
                              (sec)       (ms)      Cnt Num
0  192.168.1.130 Ser0/0        12  00:15:37 40    1000 0  10
```

3. Tabla de enrutamiento:

   - Se completa la comprobación con la verificación de las tablas de enrutamiento, donde se observan las redes publicadas.

```
LIMA#sh ip route
Gateway of last resort is not set
    192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/2172416] via 192.168.1.99, 00:09:41, Serial0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:09:55, Serial0/1
C       192.168.1.96 is directly connected, Serial0/0
C       192.168.1.128 is directly connected, Serial0/1
```

```
CHICLAYO#sh ip route
Gateway of last resort is not set
    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 00:10:18, Serial0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 00:10:18, Serial0/0
C       192.168.1.96 is directly connected, Serial0/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 00:10:18, Serial0/0
```

```
CUZCO#sh ip route
Gateway of last resort is not set
    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 00:14:36, Serial0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:14:22, Serial0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 00:14:36, Serial0/0
C       192.168.1.128 is directly connected, Serial0/0
```

4. Diagnóstico:
   - Todos los puntos de la red se pueden ver y tienen conectividad entre sí, sin restricción alguna.
   - La prueba se realiza desde un Host de red Lan del router Cuzco, primero a la Lan de Chiclayo y luego al servidor.

```
C:\Users\hector>ping 192.168.1.34

Haciendo ping a 192.168.1.34 con 32 bytes de datos:

Respuesta desde 192.168.1.34: bytes=32 tiempo=54ms TTL=125
Respuesta desde 192.168.1.34: bytes=32 tiempo=25m TTL=125
Respuesta desde 192.168.1.34: bytes=32 tiempo=35m TTL=125
Respuesta desde 192.168.1.34: bytes=32 tiempo=32m TTL=125

Estadísticas de ping para 192.168.1.34:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 25ms, Máximo = 54ms, Media = 36ms

C:\Users\hector>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:

Respuesta desde 192.168.1.2: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.1.2: bytes=32 tiempo=24 TTL=126
Respuesta desde 192.168.1.2: bytes=32 tiempo=20m TTL=126
Respuesta desde 192.168.1.2: bytes=32 tiempo=34m TTL=126

Estadísticas de ping para 192.168.1.2:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 20ms, Máximo = 34ms, Media = 25ms

C:\Users\hector>
```

FASE 4: CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO:

Debido a la solicitud del jefe de redes, a continuación se procederá a configurar las listas de control de acceso (ACL) a los routers, que es la seguridad a implementarse en la red, ya que cualquier usuario de ella en estos momentos tiene acceso a todos sus dispositivos y estaciones de trabajo.

Las siguientes condiciones serán tomadas en cuenta durante la creación de las listas de control de acceso:

- Cada router debe poder hacer Telnet en los demás routers y tener acceso a cualquier dispositivo en la red.
- El equipo WS1 y el servidor se encuentran en la subred de administración. Sólo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
- Las estaciones de trabajo en las Lan de Chiclayo y Cuzco no deben tener acceso a ningún dispositivo fuera de su subred, salvo para interconectarse con el servidor.

Teniendo en cuenta estas consideraciones, se entiende que deberá restringirse el acceso a ciertas partes de la red, para así establecer un trabajo óptimo y seguro de todos los usuarios de ésta.

Para poder entender estas consideraciones veremos el gráfico siguiente, donde mostraremos los accesos a los equipos, según lo especificado.

- Asignación de comandos para la configuración de listas de control de acceso (ACL) (desde la consola)
  - Router Cuzco y Chiclayo

```
access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
access-list 110 permit icmp any any echo-reply
access-list 110 deny   ip any any
int fast0/0
ip access-group 110 in
```

  - Router Lima

```
access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
access-list 110 deny   ip any any
int fast0/0
ip access-group 110 out
```

Con estos comandos restringimos algunos accesos. Los encargados de dar los accesos a los diferentes Hosts y dispositivos de la red son los routers, a los cuales se les ha asignado una serie de comandos que se encargarán de verificar estos accesos.

FASE 5: COMPROBACIÓN DE LA RED INSTALADA:

Después de configurar los routers probaremos las listas de control de acceso (ACL), las cuales hacen funcionar la red de la manera solicitada, para lo cual mostraremos a continuación una lista de condiciones de prueba que confirman el óptimo funcionamiento de la red.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router CHICLAYO	Router CUZCO	CORRECTO
	WS_1	Router LIMA	
	Servidor	Router CUZCO	
	Servidor	Router CHICLAYO	
TELNET	LAN del router CHICLAYO	Router CUZCO	FALLIDO
	LAN del router CUZCO	Router CUZCO	
	LAN del router CHICLAYO	Router CHICLAYO	
	LAN del router CUZCO	Router CHICLAYO	
PING	LAN del router CUZCO	WS_1	FALLIDO
	LAN del router CHICLAYO	WS_1	
	LAN del router CHICLAYO	LAN del router CUZCO	
PING	LAN del router CUZCO	Servidor	CORRECTO
	LAN del router CHICLAYO	Servidor	
	Servidor	LAN del router CHICLAYO	
	Servidor	LAN del router CUZCO	
	Router CUZCO	LAN del router CHICLAYO	
	Router CHICLAYO	LAN del router CUZCO	

- De esta manera se demuestra que la configuración establecida en los routers y Hosts de nuestra red se realizó de manera satisfactoria, con lo que su funcionamiento será óptimo y trabajará según lo solicitado.

FASE 6: CONFIGURACIÓN FINAL

- Para efectos de apoyo y para simplificar el diagnóstico de fallas, mostraremos a continuación de forma organizada y lógica las siguientes visualizaciones:

```
LIMA#sh runn
Building configuration...
Current configuration : 1157 bytes
!
version 12.2
no service password-encryption
!
hostname LIMA
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
ip ssh version 1
ip host CHICLAYO 192.168.1.99 192.168.1.33
ip host CUZCO 192.168.1.131 192.168.1.65
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
 ip access-group 110 out
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 192.168.1.98 255.255.255.224
!
interface Serial0/1
 ip address 192.168.1.130 255.255.255.224
 clock rate 64000
!
!
router eigrp 200
 network 192.168.1.0 0.0.0.31
 network 192.168.1.96 0.0.0.31
 network 192.168.1.128 0.0.0.31
 no auto-summary
!
ip classless
!
!
access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
access-list 110 deny ip any any
!
!
```

```
CUZCO#sh run
Building configuration...
Current configuration : 1157 bytes
!
version 12.2
no service password-encryption
!
hostname CUZCO
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
ip ssh version 1
ip host CHICLAYO 192.168.1.99 192.168.1.33
ip host LIMA 192.168.1.130 192.168.1.1
!
!
interface FastEthernet0/0
 ip address 192.168.1.65 255.255.255.224
 ip access-group 110 in
 duplex auto
 speed auto
!
!
interface Serial0/0
 ip address 192.168.1.131 255.255.255.224
!
!
router eigrp 200
 network 192.168.1.128 0.0.0.31
 network 192.168.1.64 0.0.0.31
 no auto-summary
!
ip classless
!
!
access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
access-list 110 permit icmp any any echo-reply
access-list 110 deny ip any any
!
!
```

```
CHICLAYO#sh run
Building configuration...

Current configuration : 1073 bytes
!
version 12.2
no service password-encryption
!
hostname CHICLAYO
!
!
```

```
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
ip ssh version 1
ip host CUZCO 192.168.1.131 192.168.1.65
ip host LIMA 192.168.1.130 192.168.1.1
!
!
interface FastEthernet0/0
 ip address 192.168.1.33 255.255.255.224
 ip access-group 110 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 192.168.1.99 255.255.255.224
 clock rate 64000
!
!
interface FastEthernet1/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
router eigrp 200
 network 192.168.1.32 0.0.0.31
 network 192.168.1.96 0.0.0.31
 no auto-summary
!
ip classless
!
!
access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
access-list 110 permit icmp any any echo-reply
access-list 110 deny ip any any
!
!
```

OBSERVACIONES Y/O COMENTARIOS

LABORATORIO N° 7 - CONEXIÓN DE VLAN INALÁMBRICA Y EL PUENTE COMO RUTA DE RESPALDO

INTRODUCCIÓN

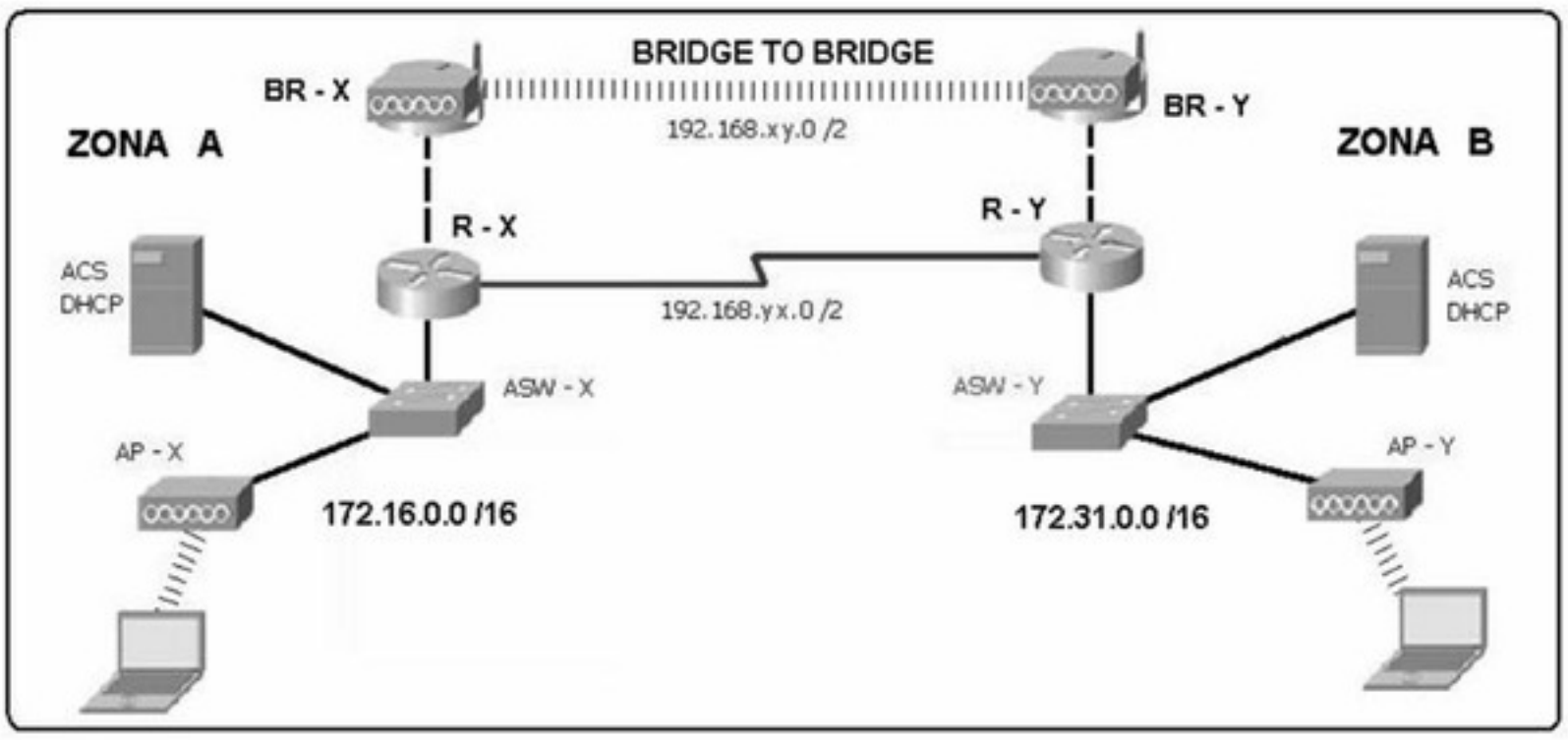
Para proporcionar a los empleados la cobertura inalámbrica más completa, necesita instalar puntos de acceso en su oficina o almacén. Los puntos de acceso de Cisco Aironet 1130AG Series y Cisco Aironet 1240AG Series proporcionan varias ventajas con respecto a las exigencias actuales, como son los servicios de seguridad, rendimiento y movilidad que necesita. Incluso se pueden complementar con equipos como un switch router Cisco.

OBJETIVOS

- Implementación de un puente en conexión bridge to bridge.
- Implementación de un access point con VLAN inalámbricas.
- Habilitar la autenticación de dispositivos en un servidor TACACS+.

DESCRIPCIÓN

En el siguiente diagrama de red se presentan dos sucursales de una entidad con la misma configuración interna. Lo que se necesita es que las VLAN definidas en el switch se propaguen mediante el access point (AP) con la opciones de seguridad indicadas. El enlace WAN entre ambas sucursales (interfaces seriales) debe tener un enlace inalámbrico de respaldo.



Implementar la topología indicada en el diagrama con los siguientes requerimientos:

1. Resuelva el direccionamiento IP asignado a las redes indicadas.
2. Cree las VLAN indicadas en el diagrama empleando el router para intervlan.
3. Configure el enlace bridge to bridge como respaldo del enlace WAN con protección WEP.
4. Defina el protocolo de enrutamiento dinámico a emplear.
5. El ACS y el servidor DHCP se encuentran en la VLAN de servidores.
6. Las VLAN 20, 30 y 40 deben ser propagadas sobre la red wireless, con la seguridad indicada.

VLAN	CARACTERÍSTICAS
1	NATIVE /ADMINISTRACIÓN
10	VOICE
20	DATA1 /WEP
30	DATA2 /LEAP
40	GUEST / OPEN

7. Configure AAA en todos los equipos para que el acceso a ellos sea autenticado en el servidor TACACS+.
8. Los clientes deberán emplear NIC genérica y NIC Cisco.

DESARROLLO

IMPLEMENTACIÓN DE LA ZONA A:

1. **CONFIGURACIÓN DEL ROUTER**

- Asignación de direcciones IP en interfaces y subinterfaces de acuerdo a lo establecido en el direccionamiento, además del encapsulamiento a cada subinterfaz.

Interfaz	Dirección IP	Encapsulamiento dot1q /VLAN
FastEthernet0/0	192.168.12.1/24	----------
FastEthernet0/1.1	172.16.1.1/24	1 native
FastEthernet0/1.10	172.16.10.1/24	10
FastEthernet0/1.20	172.16.20.1/24	20
FastEthernet0/1.30	172.16.30.1/24	30
FastEthernet0/1.40	172.16.40.1/24	40
FastEthernet0/1.50	172.16.50.1/24	50
Serial0/0/1	192.168.21.1/24	--------

- Habilitar el enrutamiento mediante EIGRP, donde se incluye cada una de las subredes y el enlace WAN. Aquí no se contempla la red de conexión mediante el puente.

```
router eigrp 1
 network 172.16.1.0 0.0.0.255
 network 172.16.10.0 0.0.0.255
 network 172.16.16.0 0.0.0.255
 network 172.16.20.0 0.0.0.255
 network 172.16.30.0 0.0.0.255
 network 172.16.40.0 0.0.0.255
 network 172.16.50.0 0.0.0.255
 network 192.168.21.0
 no auto-summary
```

- Habilitar una ruta estática como backup de EIGRP. Obsérvese que la distancia administrativa se ha modificado para permitir que las rutas EIGRP sean las preferidas para alcanzar la red 192.168.12.0.

```
ip route 172.31.0.0 255.255.0.0 192.168.12.3 150
```

- Habilitar en las subinterfaces el tráfico de mensajes broadcast hacia el servidor DHCP, para que los clientes de las VLAN puedan recibir una dirección IP desde el servidor DHCP.

```
ip helper address 10.30.30.2
ip helper address 172.16.50.2
```

- Indicar el servidor de autenticación TACACS+, así como definir el grupo para la autenticación del terminal virtual (TELNET).

```
aaa new-model
! !
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
tacacs-server host 172.16.50.2 key cisco123
```

- Habilitar la autenticación para el acceso vía el terminal virtual (Telnet).

```
line vty 0 4
 password cisco
 login authentication TELNET
```

2. A continuación, se muestra la configuración final en el router:

```
R1#sh run
Building configuration...
Current configuration : 2436 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$6OTj$F1ejoZdCa1vG43MnJWhfU/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
!
aaa session-id common
!
 resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
```

```
!
!
no ip dhcp use vrf connected
!
!
!
username cisco privilege 15 password 0 cisco
!
!
!
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 10.3.3.2
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 10.30.30.2
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.16.20.1 255.255.255.0
 ip helper-address 10.30.30.2
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.16.30.1 255.255.255.0
 ip helper-address 10.30.30.2
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface FastEthernet0/1.40
 encapsulation dot1Q 40
 ip address 172.16.40.1 255.255.255.0
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface FastEthernet0/1.50
 encapsulation dot1Q 50
```

```
 ip address 172.16.50.1 255.255.255.0
 ip helper-address 172.16.50.2
 no snmp trap link-status
!
interface Serial0/0/0
 no ip address
 clockrate 64000
!
interface Serial0/0/1
 ip address 192.168.21.1 255.255.255.0
 clockrate 64000
!
router eigrp 1
 network 172.16.1.0 0.0.0.255
 network 172.16.10.0 0.0.0.255
 network 172.16.16.0 0.0.0.255
 network 172.16.20.0 0.0.0.255
 network 172.16.30.0 0.0.0.255
 network 172.16.40.0 0.0.0.255
 network 172.16.50.0 0.0.0.255
 network 192.168.21.0
 no auto-summary
!
ip classless
ip route 172.31.0.0 255.255.0.0 192.168.12.3 150
!
no ip http server
!
tacacs-server host 172.16.50.2 key cisco123
tacacs-server directed-request
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login authentication TELNET
!
end
```

3. La tabla de enrutamiento en el router indicará todas las redes aprendidas desde el router vecino:

```
R1# sh ip route
Gateway of last resort is not set
C   192.168.12.0/24 is directly connected, FastEthernet0/0
    172.16.0.0/24 is subnetted, 6 subnets
C      172.16.50.0 is directly connected, FastEthernet0/1.50
C      172.16.40.0 is directly connected, FastEthernet0/1.40
C      172.16.30.0 is directly connected, FastEthernet0/1.30
C      172.16.20.0 is directly connected, FastEthernet0/1.20
C      172.16.10.0 is directly connected, FastEthernet0/1.10
C      172.16.1.0 is directly connected, FastEthernet0/1.1
    172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
```

```
D     172.31.3.0/24 [90/20514560] via 192.168.21.2, 00:03:04, Serial0/0/1
D     172.31.2.0/24 [90/20514560] via 192.168.21.2, 00:03:04, Serial0/0/1
D     172.31.1.0/24 [90/20514560] via 192.168.21.2, 00:03:04, Serial0/0/1
S     172.31.0.0/16 [150/0] via 192.168.12.3
 D     172.31.6.0/24 [90/20514560] via 192.168.21.2, 00:03:04, Serial0/0/1
 D     172.31.5.0/24 [90/20514560] via 192.168.21.2, 00:03:05, Serial0/0/1
 D     172.31.4.0/24 [90/20514560] via 192.168.21.2, 00:03:05, Serial0/0/1
 C   192.168.21.0/24 is directly connected, Serial0/0/1
R1#
```

4. CONFIGURACIÓN DEL SWITCH

- Asignación de direcciones IP de acuerdo a la configuración establecida:

```
interface Vlan1
 ip address 172.16.1.2 255.255.255.0
```

- Configuración de VLAN, enlaces troncales, asignación de puertos con algunas características de seguridad (dot1x) y facilidad de conexión (portfast).

VLAN	PUERTOS	OTRO
10	0/1	dot1x port-control auto
	0/2	
20	0/3	dot1x port-control auto
	0/4	
30	0/5 - 6	dot1x port-control auto, spanning-tree portfast
40	0/7 - 8	
50	0/9 – 10	
TRUNK	0/11 - 12	

- Indicar el servidor de autenticación TACACS.

```
tacacs-server host 172.16.50.2 key cisco123
```

- Habilitar la autenticación para el acceso vía el terminal virtual (Telnet).

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
!
line vty 0 15
 password cisco
 login authentication TELNET
```

- Habilitar la autenticación dot1x para los puertos.

```
aaa authentication dot1x default group tacacs+
dot1x system-auth-control
```

- A continuación se muestra la configuración final en el switch:

```
SW-1#sh runn
Building configuration...
Current configuration : 2058 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW-1
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
aaa authentication dot1x default group tacacs+
enable secret 5 $1$iMfy$aqR5PexsNQFTCF8JT7czR.
!
username cisco privilege 15 password 0 cisco
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 dot1x port-control auto
!
 interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
 dot1x port-control auto
```

```
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 40
 switchport mode access
        !
interface FastEthernet0/9
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/11
 switchport trunk allowed vlan 1,10,20,30,40,50
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk allowed vlan 1,10,20,30,40,50
 switchport mode trunk
!
interface Vlan1
 ip address 172.16.1.2 255.255.255.0
 no ip route-cache
!
ip http server
tacacs-server host 172.16.50.2 key cisco123
        !
line con 0
 speed 115200
line vty 0 4
 password cisco
 login authentication TELNET
line vty 5 15
 password cisco
 login authentication TELNET
!
!
end
```

5. CONFIGURACIÓN DE AP

- Se define el rol a cumplir, de acuerdo al planteamiento; en este caso es necesario indicar que el AP debe propagar las VLAN y, a su vez, trabajar de forma totalmente independiente.

```
Station-role root
```

- Asignación de direcciones IP de acuerdo a la configuración establecida; en este equipo se habilita la interfaz BVI1 con su dirección IP.

```
interface BVI1
 ip address 172.16.1.3 255.255.255.0
```

- Configuración de VLAN y sus puertos, tanto para los enlaces inalámbricos (interfaz Dot11Radio0) como para su en lace cableado (interfaz FastEthernet 0).
- Habilitar la interfaz Dot 11 Radio 0 y la interfaz FastEthernet0, a su vez, definir las subinterfaces para cada VLAN con su encapsulamiento correspondiente.
- Debe tenerse en cuenta que al configurar de esa manera, el puerto FastEthernet se convierte en un puerto troncal, aceptando las tramas de las diferentes VLAN y, a su vez, al puerto Dot11Radio0 para el enlace inalámbrico.

VLAN	Interfaces	NOMBRE	SSID	Otros
10	Dot11Radio0.10 y FastEthernet0.10	VLAN	WMAX10	authentication open, mbssid guest-mode
20	Dot11Radio0.20 y FastEthernet0.20	VLAN20	WMAX20	authentication open, mbssid guest-mode
30	Dot11Radio0.30 y FastEthernet0.30	VLAN30	WMAX30	authentication open, mbssid guest-mode
40	Dot11Radio0.40 y FastEthernet0.40	VLAN40	WMAX40	authentication network-eap eap_methods, accounting acct_methods, mbssid guest-mode
1	Dot11Radio0.1 y FastEthernet0.1	VLAN1	WMAX1	authentication open, infrastructure-ssid optional

o Indicar el servidor de autenticación TACACS y RADIUS.

```
tacacs-server host 172.16.50.2 key 7 13061E010803557878
radius-server host 172.16.50.2 auth-port 1645 acct-port 1646 key 7 070C285F4D06485744
```

o Habilitar la autenticación para el terminal virtual (Telnet) mediante TACACS.

```
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
!
!
line vty 0 5
 login authentication TELNET
```

- Definir para cada VLAN asignada el tipo de autenticación y el modo de propagación de su SSID.

```
aaa new-model
!
!
aaa group server radius rad_eap
 server 172.16.50.2 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
 server 172.16.50.2 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tacacs+ local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
```

- A continuación se muestra la configuración final en el access point:

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$.RYi$TKfONwRHKbudkabQ/uXVS.
!
!
ip subnet-zero
ip domain name ap2.com
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 172.16.50.2 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
 server 172.16.50.2 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
!
```

```
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tacacs+ local
aaa authentication login TELNET group tacacs+ local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
dot11 vlan-name VLAN vlan 10
dot11 vlan-name VLAN1 vlan 1
dot11 vlan-name VLAN20 vlan 20
dot11 vlan-name VLAN30 vlan 30
dot11 vlan-name VLAN40 vlan 40
!
dot11 ssid WMAX1
  vlan 1
  authentication open
  infrastructure-ssid optional
!
dot11 ssid WMAX10
  vlan 10
  authentication open
  mbssid guest-mode
!
dot11 ssid WMAX20
  vlan 20
  authentication open
  mbssid guest-mode
!
dot11 ssid WMAX30
  vlan 30
  authentication network-eap eap_methods
  accounting acct_methods
  mbssid guest-mode
!
dot11 ssid WMAX40
  vlan 40
  authentication open
  mbssid guest-mode
!
!
!
username Cisco privilege 15 password 7 00071A150754
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
```

```
encryption vlan 20 key 1 size 128bit 7 4A056E3B5EFA156E346C961F0744 transmit-key
encryption vlan 20 mode ciphers wep128
!
encryption vlan 30 mode wep mandatory
!
ssid WMAX1
!
ssid WMAX10
!
ssid WMAX20
!
ssid WMAX30
!
ssid WMAX40
!
mbssid
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
 bridge-group 10 subscriber-loop-control
 bridge-group 10 block-unknown-source
 no bridge-group 10 source-learning
 no bridge-group 10 unicast-flooding
 bridge-group 10 spanning-disabled
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
```

```
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 dfs band 3 block
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 hold-queue 160 in
!
interface FastEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
 no bridge-group 10 source-learning
 bridge-group 10 spanning-disabled
!
interface FastEthernet0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 no bridge-group 20 source-learning
 bridge-group 20 spanning-disabled
!
```

```
interface FastEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
!
interface BVI1
 ip address 172.16.1.3 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 172.16.50.2 key 7 13061E010803557878
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 172.16.50.2 auth-port 1645 acct-port 1646 key 7 070C285F4D06485744
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 5
 login authentication TELNET
!
```

6. CONFIGURACION DEL PUENTE

- Se debe considerar que el puente es un dispositivo de respaldo en este caso y, por lo tanto, debe permitir que todas las VLAN también pasen su tráfico por esa vía pero, a diferencia del access point, el puente sólo transmite al otro puente, por lo que deberá ser como una especie de enlace troncal. Al comunicarse dos puentes, uno deberá ser **root bridge** (el equipo de la zona A) y el otro puente se configurará como **non-root bridge**.

```
station-role root bridge
```

- Se asigna la dirección IP que va a tener la interfaz del puente, tanto para su enlace cableado como inalámbrico.

```
interface BVI1
 ip address 192.168.12.2 255.255.255.0
```

- Asignar el nombre a la VLAN 1.

```
dot11 vlan-name vlan1 vlan 1
```

- Definir el SSID que se empleará en la VLAN 1 (UTP) para la comunicación de los puentes, la autenticación y el modo de trabajo.

```
dot11 ssid UTP
  vlan 1
  authentication open
  infrastructure-ssid
```

- Deberán crearse subinterfaces tanto en la FastEthernet 0 como en Dot11Radio0 para la VLAN 1.

```
interface FastEthernet0.1
 encapsulation dot1Q 1 native
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
```

- El enlace bridge to bridge deberá tener protección WEP.

```
encryption vlan 1 key 1 size 128bit 7 3A1E467E23EAD518A21653687A42 transmit-key
 encryption vlan 1 mode wep mandatory
```

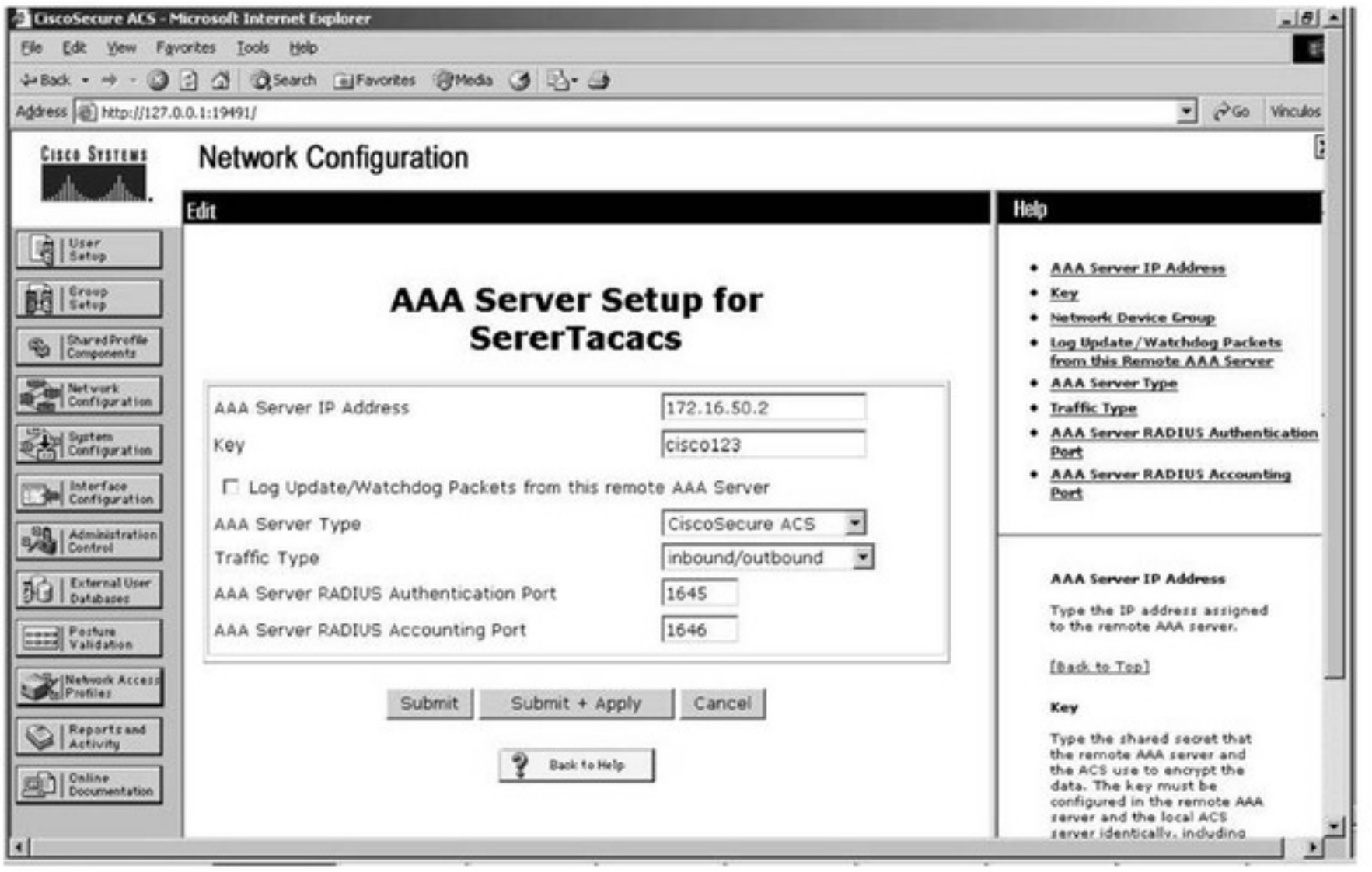
- A continuación se muestra la configuración final en el puente (bridge):

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BR1
!
enable secret 5 $1$pERK$65hffLyGQnPolsrwH9pRS1
!
ip subnet-zero
ip domain name cisco.com
!
!
no aaa new-model
dot11 vlan-name vlan1 vlan 1
!
dot11 ssid UTP
  vlan 1
  authentication open
  infrastructure-ssid
!
!
!
username Cisco password 7 02250D480809
!
bridge irb
!
```

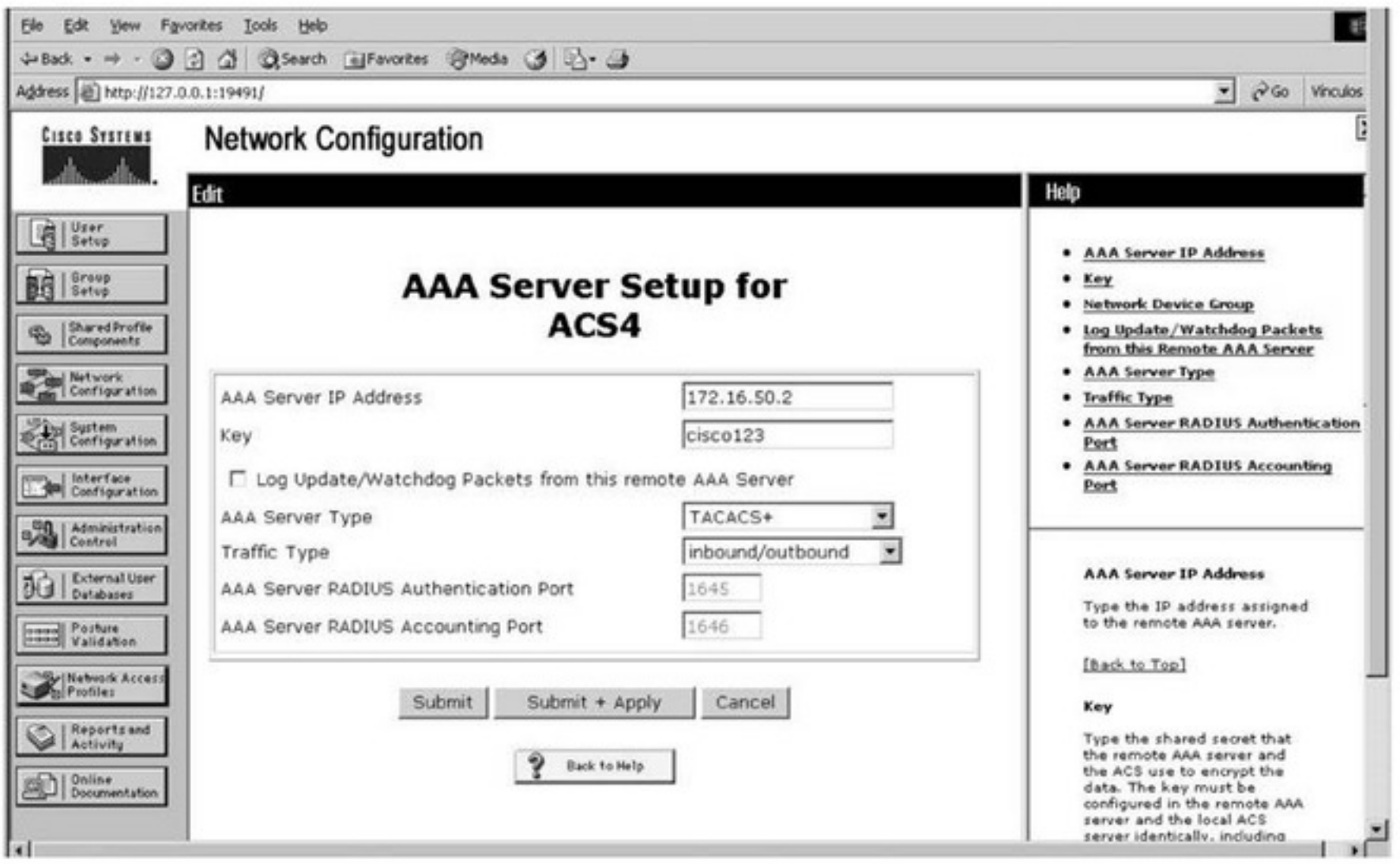
```
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 1 key 1 size 128bit 7 3A1E467E23EAD518A21653687A42 transmit-key
 encryption vlan 1 mode wep mandatory
 !
 ssid UTP
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root bridge
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 hold-queue 80 in
!
interface FastEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.12.2 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 login local
!
end
```

7. CONFIGURACIÓN DEL ACS

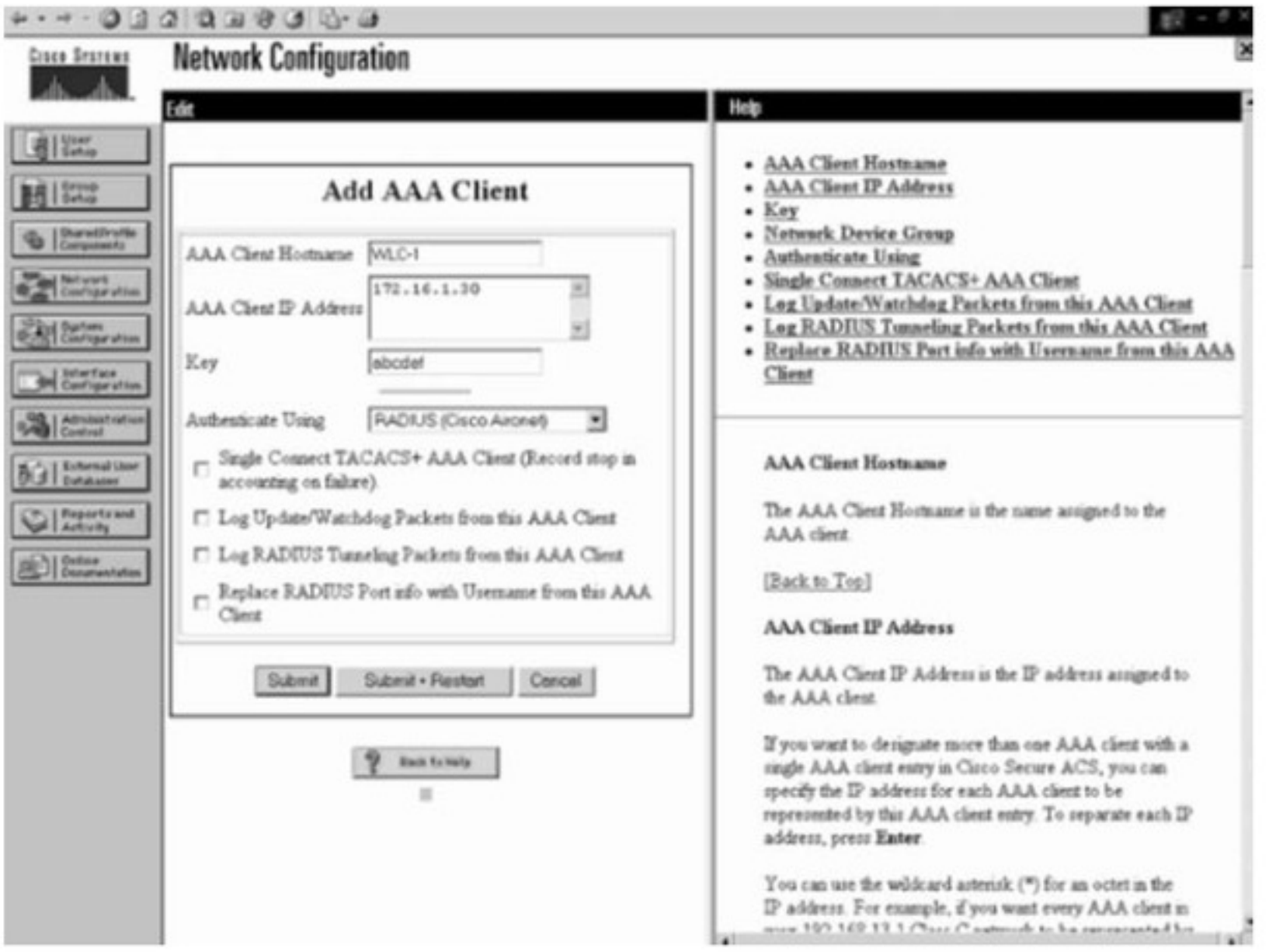
- Definiendo el servidor RADIUS en el ACS, donde se asigna el IP 172.16.50.2 y la clase cisco123, los siguientes son parámetros comunes de configuración:

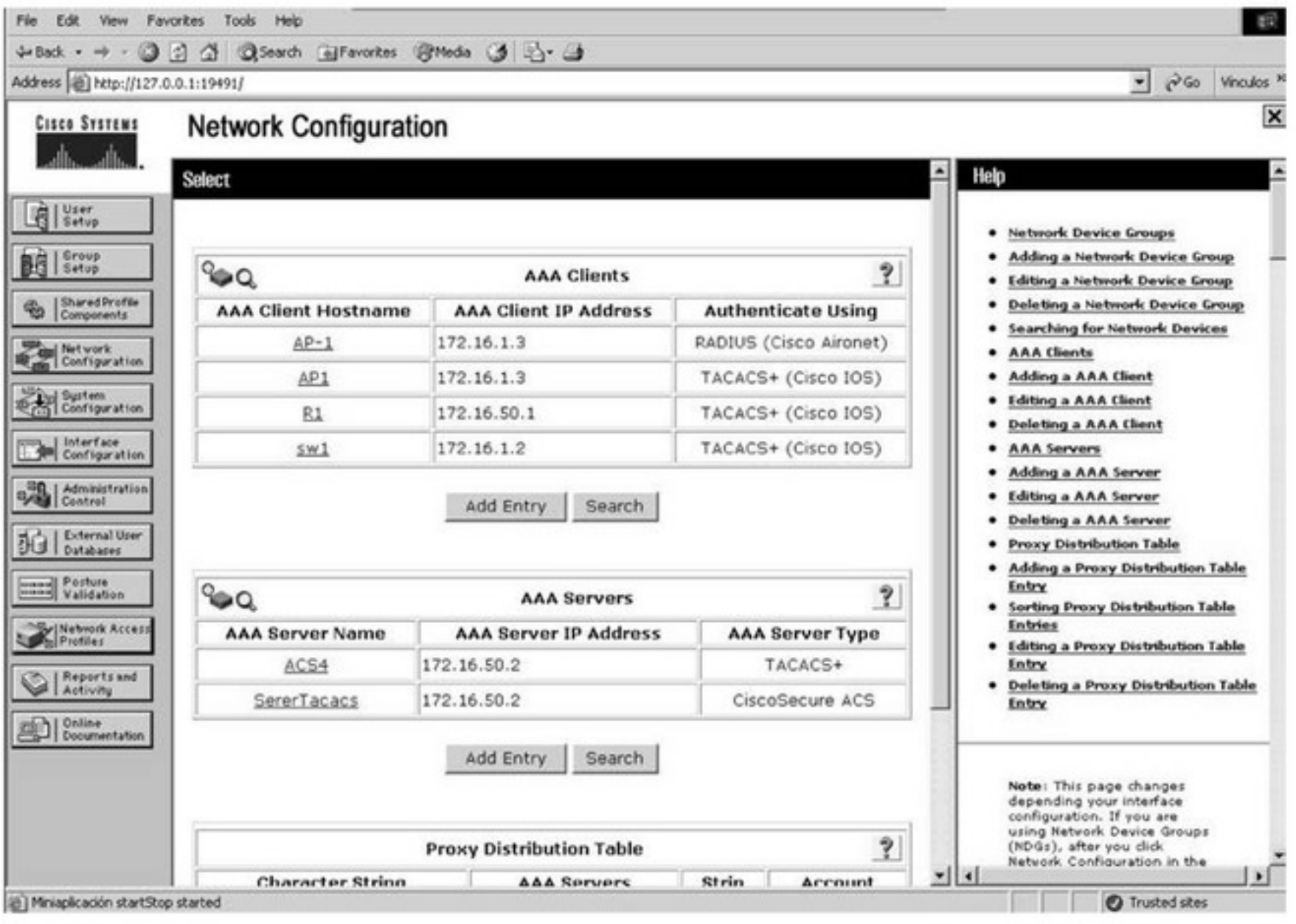

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://127.0.0.1:19491/
Network Configuration
Edit
AAA Server Setup for SererTacacs
AAA Server IP Address 172.16.50.2
Key cisco123
Log Update/Watchdog Packets from this remote AAA Server
AAA Server Type CiscoSecure ACS
Traffic Type inbound/outbound
AAA Server RADIUS Authentication Port 1645
AAA Server RADIUS Accounting Port 1646
Submit
Submit + Apply
Cancel
Back to Help
Help
AAA Server IP Address
Key
Network Device Group
Log Update/Watchdog Packets from this Remote AAA Server
AAA Server Type
Traffic Type
AAA Server RADIUS Authentication Port
AAA Server RADIUS Accounting Port
AAA Server IP Address
Type the IP address assigned to the remote AAA server.
[Back to Top]
Key
Type the shared secret that the remote AAA server and the ACS use to encrypt the data. The key must be configured in the remote AAA server and the local ACS

- Definiendo el servidor TACACS en el ACS, donde se asigna el mismo IP 172.16.50.2 (ya que están en el mismo servidor) y la clase cisco123, los siguientes son parámetros comunes de configuración:

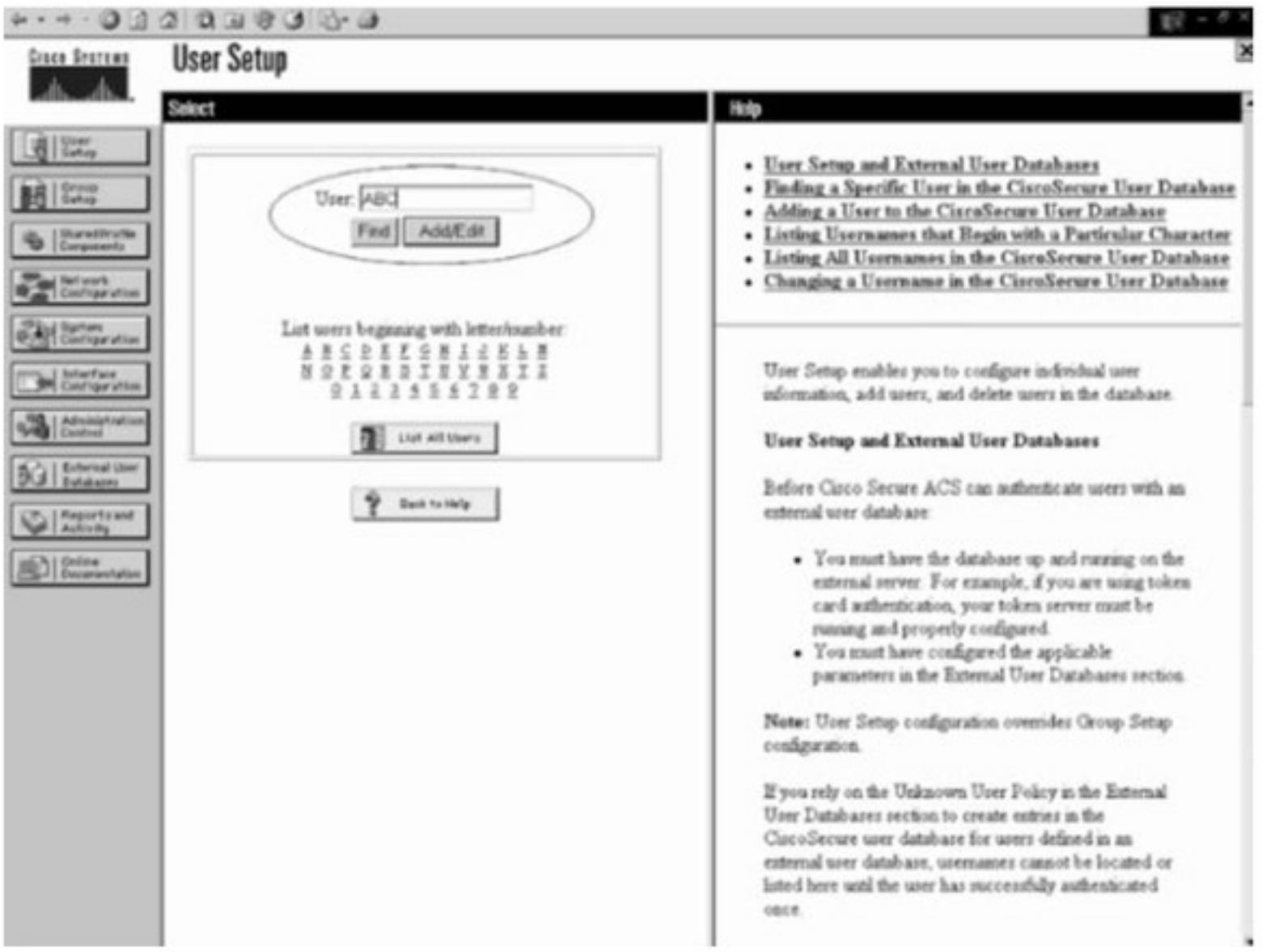

File Edit View Favorites Tools Help
Address http://127.0.0.1:19491/
Network Configuration
Edit
AAA Server Setup for ACS4
AAA Server IP Address 172.16.50.2
Key cisco123
Log Update/Watchdog Packets from this remote AAA Server
AAA Server Type TACACS+
Traffic Type inbound/outbound
AAA Server RADIUS Authentication Port 1645
AAA Server RADIUS Accounting Port 1646
Submit
Submit + Apply
Cancel
Back to Help
Help
AAA Server IP Address
Key
Network Device Group
Log Update/Watchdog Packets from this Remote AAA Server
AAA Server Type
Traffic Type
AAA Server RADIUS Authentication Port
AAA Server RADIUS Accounting Port
AAA Server IP Address
Type the IP address assigned to the remote AAA server.
[Back to Top]
Key
Type the shared secret that the remote AAA server and the ACS use to encrypt the data. The key must be configured in the remote AAA server and the local ACS

- En la siguiente secuencia se configuran los equipos que van a emplear la autenticación, en este caso, se debe definir el nombre y su dirección IP.

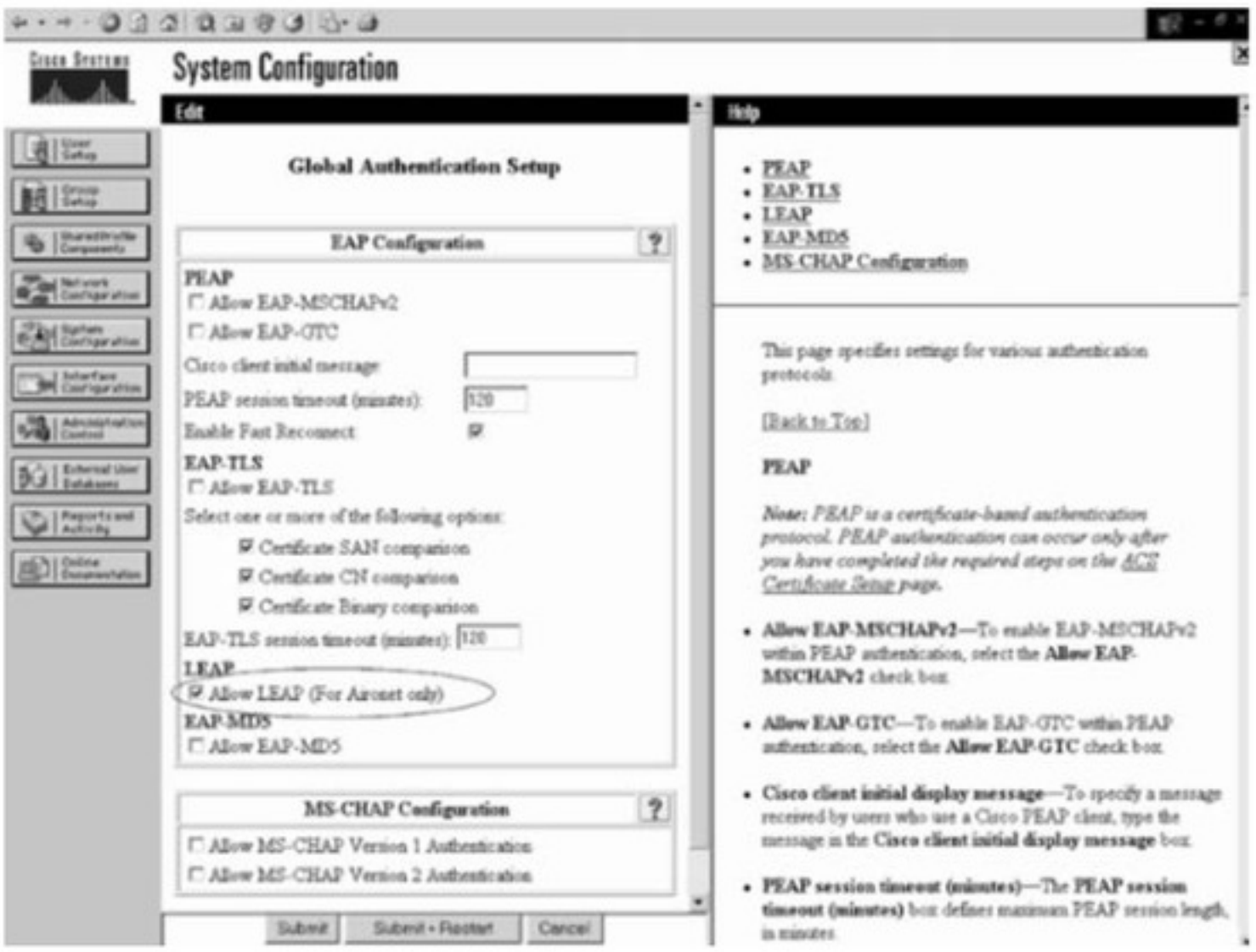

Network Configuration
Edit
Add AAA Client
AAA Client Hostname
WLC-1
AAA Client IP Address
172.16.1.30
Key
abcdef
Authenticate Using
RADIUS (Cisco Aironet)
Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
Log Update/Watchdog Packets from this AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Replace RADIUS Port info with Username from this AAA Client
Submit
Submit + Restart
Cancel
Back to Help
Help
AAA Client Hostname
AAA Client IP Address
Key
Network Device Group
Authenticate Using
Single Connect TACACS+ AAA Client
Log Update/Watchdog Packets from this AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Replace RADIUS Port info with Username from this AAA Client
AAA Client Hostname
The AAA Client Hostname is the name assigned to the AAA client.
[Back to Top]
AAA Client IP Address
The AAA Client IP Address is the IP address assigned to the AAA client.
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in



- Finalmente, en la opción **user Setup**, configure los usuarios que deberán autenticarse junto con su contraseña.

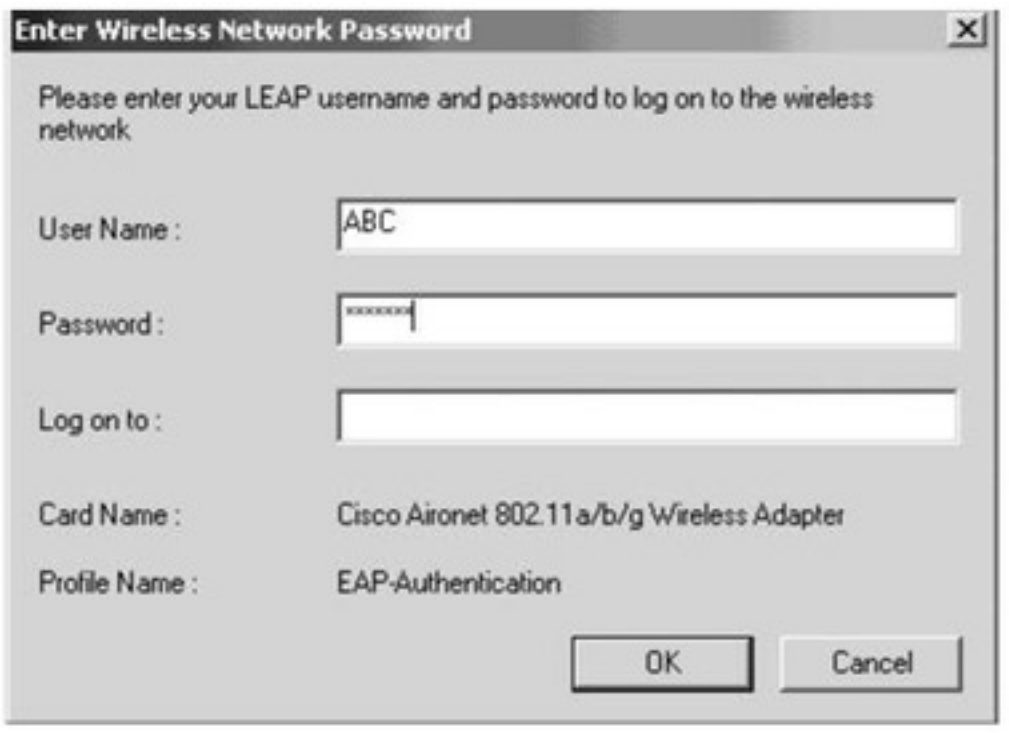

User Setup
Select
User: ABC
Find
Add/Edit
List users beginning with letter/number:
List All Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the CiscoSecure User Database
Adding a User to the CiscoSecure User Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the CiscoSecure User Database
Changing a Username in the CiscoSecure User Database
User Setup enables you to configure individual user information, add users, and delete users in the database.
User Setup and External User Databases
Before Cisco Secure ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the CiscoSecure user database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

- Haga clic en **System Configuration** y **Global Authentication Setup** con el fin de garantizar que el servidor de autenticación esté configurado para realizar el método de autenticación EAP. Elija el método adecuado de EAP. En este ejemplo se utiliza la autenticación LEAP. Haga clic en **Submit** cuando haya terminado.


System Configuration
Edit
Global Authentication Setup
EAP Configuration
PEAP
Allow EAP-MSCHAPv2
Allow EAP-GTC
Cisco client initial message:
PEAP session timeout (minutes): 120
Enable Fast Reconnect
EAP-TLS
Allow EAP-TLS
Select one or more of the following options:
Certificate SAN comparison
Certificate CN comparison
Certificate Binary comparison
EAP-TLS session timeout (minutes): 120
LEAP
Allow LEAP (For Aironet only)
EAP-MD5
Allow EAP-MD5
MS-CHAP Configuration
Allow MS-CHAP Version 1 Authentication
Allow MS-CHAP Version 2 Authentication
Submit
Submit + Restart
Cancel
Help
PEAP
EAP-TLS
LEAP
EAP-MD5
MS-CHAP Configuration
This page specifies settings for various authentication protocols.
[Back to Top]
PEAP
Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.
Allow EAP-MSCHAPv2—To enable EAP-MSCHAPv2 within PEAP authentication, select the Allow EAP-MSCHAPv2 check box.
Allow EAP-GTC—To enable EAP-GTC within PEAP authentication, select the Allow EAP-GTC check box.
Cisco client initial display message—To specify a message received by users who use a Cisco PEAP client, type the message in the Cisco client initial display message box.
PEAP session timeout (minutes)—The PEAP session timeout (minutes) box defines maximum PEAP session length, in minutes.

8. **VERIFICACIÓN**

- Al momento de acceder a la red de la VLAN 30 aparece la ventana que se muestra, donde se deberá colocar el usuario y la contraseña registrada.



CONCLUSIONES

_____

_____

LABORATORIO N° 8

INTRODUCCIÓN

Los esquemas de red en ciertas circunstancias son similares y pueden permitir que una solución funcione sin problemas, con ciertas adaptaciones, como el caso de las listas de control de acceso, el servicio DHCP, el enrutamiento con autenticación, entre otros.

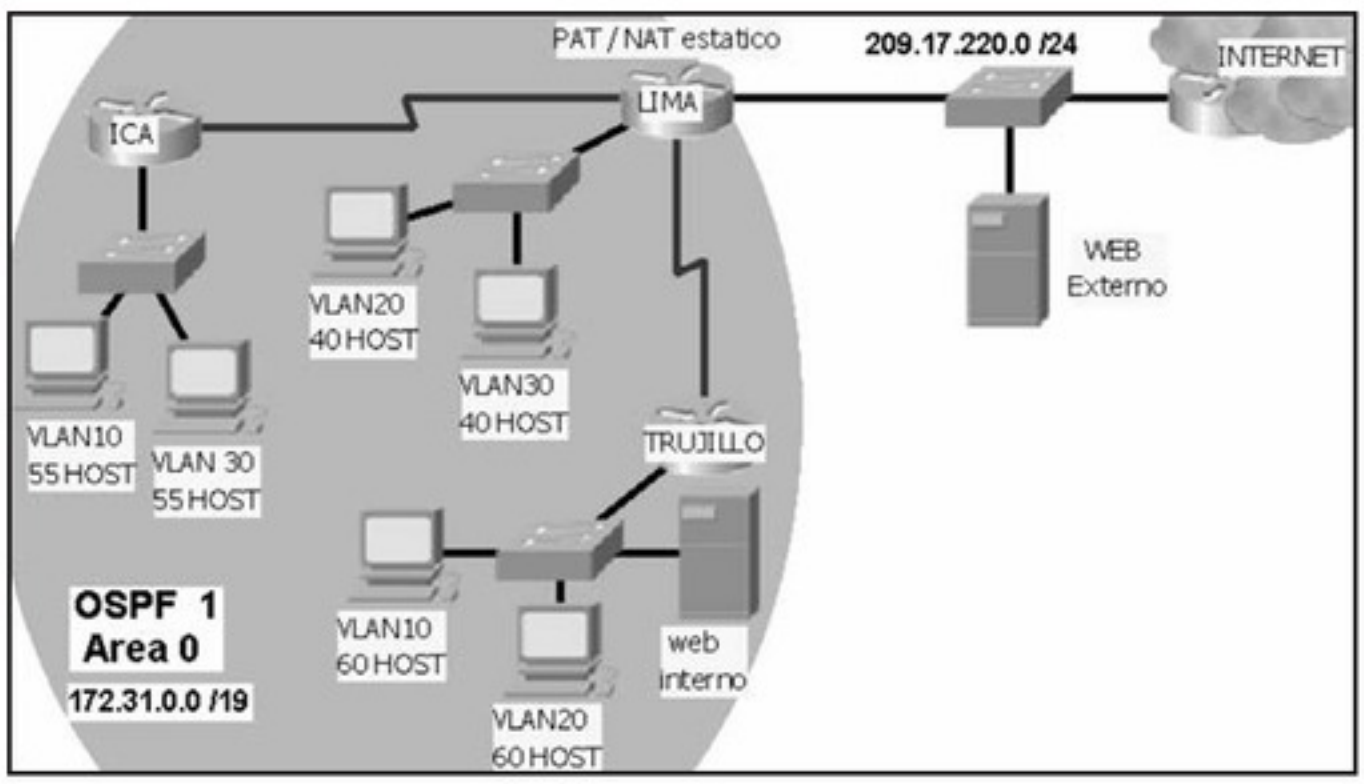
En una topología se permite diferenciar las características de los diferentes servicios que presenta un router e integrar soluciones que deberán complementarse para facilitar el trabajo en conjunto y cumplir los requerimientos.

OBJETIVO

- Implementación de servicios en los routers que permitan integrar soluciones para el caso planteado.

DESCRIPCIÓN

El esquema siguiente es un caso típico que presenta una empresa al tener la conexión a Internet en una red Ethernet, la cual debe adaptarse para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a Internet pero empleando las direcciones de la red Lan original.



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener lo siguiente:
   - Configuración básica.
   - Autenticación local con AAA.
   - Cifrado de contraseñas.
   - Un máximo de intentos para acceder al router.
   - Máximo tiempo de acceso al detectar ataques.
   - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

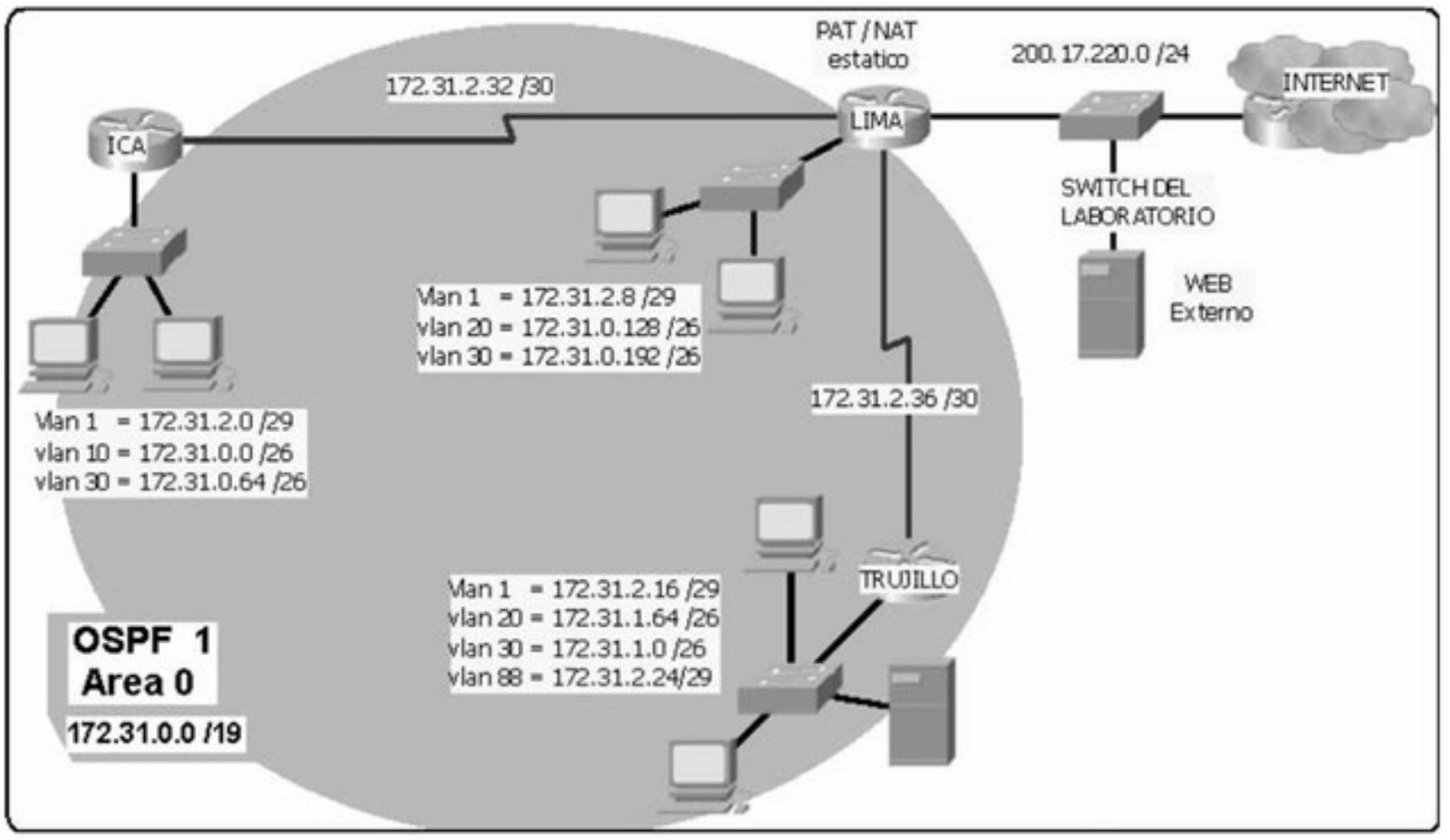
2. El DHCP deberá proporcionar sólo direcciones a los Hosts de Ica y Trujillo.
3. El web server deberá tener NAT estático y el resto de equipos de la topología emplearán NAT de sobrecarga (PAT).
4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:
   - Los Hosts de VLAN 20 en Trujillo no acceden a Internet, sólo a la red interna de Lima e Ica.
   - Los Hosts de VLAN 10 en Trujillo sí acceden a Internet y no a la red interna de Lima e Ica.
   - Los Hosts de VLAN 30 en Lima sólo acceden a servidores web y ftp de Internet.
   - Los Hosts de VLAN 20 en Lima sólo acceden a la VLAN 20 de Trujillo y VLAN 10 de Ica.
   - Los Hosts de VLAN 30 en Ica acceden a Internet y a cualquier equipo de la VLAN 10.
   - Los Hosts de VLAN 10 en ICA acceden a la red de Trujillo (vlan 20) y LIMA(vlan20), no Internet
   - Los Hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
   - Sólo los Hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e Internet.
6. VLSM: Utilizar la dirección 172.31.0.0/18 para el direccionamiento.

DESARROLLO

Se determinó configurar los siguientes servicios para permitir el desarrollo del planteamiento:

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Lima, mediante el helper address, para los routers Ica y Trujillo.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo a los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual.

1. El diagrama describe la solución para el direccionamiento requerido:



2. **AUTENTICACIÓN**:

- Se habilita AAA en el equipo y se crea una lista con el perfil del grupo a autenticarse (LOCAL_AUTH); para este caso será local, es decir, con usuarios registrados en el equipo.

```
aaa new-model
aaa authentication login LOCAL_AUTH local
```

- Configuración de consola.

```
exec-timeout 5 0
 logging synchronous
 login
 login authentication LOCAL_AUTH
```

- Configuración de terminal virtual.

```
exec-timeout 5 0
 login
 login authentication LOCAL_AUTH
```

- Usuarios registrados en todos los routers.

```
username LIMA privilege 7 password 0 network
username uica password 0 uica
username ulima password 0 ulima
username utrujillo password 0 utrujillo
```

- Un máximo de intentos para acceder al router.

  Máximo tiempo de acceso al detectar ataques.

  Para dificultar los intentos de conexión forzada, durante cuatro minutos el router se bloqueará (240 segundos), con un máximo de cinco intentos (rate 5 log) en dos minutos.

```
login block for 240 attempts 4 within 120
security authentication failure rate 5 log
```

3. **SERVICIO DE DHCP**

- En el router Lima se realiza la mayor configuración, para proporcionar el servicio hacia los Hosts de Ica y Trujillo.
- Exclusión de direcciones:

```
ip dhcp excluded
address 172.31.1.65 172.31.1.70
ip dhcp excluded
address 172.31.1.1 172.31.1.5
ip dhcp excluded
address 172.31.0.1 172.31.0.5
ip dhcp excluded
address 172.31.0.65 172.31.0.70
```

- Estableciendo los pools de cada VLAN:

```
ip dhcp pool ica-30
 network 172.31.0.64 255.255.255.192
 default-router 172.31.0.65
ip dhcp pool t-10
 network 172.31.1.0 255.255.255.192
 default-router 172.31.1.1
ip dhcp pool t-20
 network 172.31.1.64 255.255.255.192
 default-router 172.31.1.65
ip dhcp pool ica-10
 network 172.31.0.0 255.255.255.192
 default-router 172.31.0.1
```

- En las subinterfaces del router Ica se permite el paso de broadcast DHCP hacia el router Lima.

```
interface FastEthernet0/0.10
ip helper-address 172.31.2.34
!
interface FastEthernet0/0.30
ip helper-address 172.31.2.34
```

- En las subinterfaces del router Trujillo se permite el paso de broadcast DHCP hacia el router Lima.

```
interface FastEthernet0/0.10
ip helper-address 172.31.2.38
!
interface FastEthernet0/0.20
ip helper-address 172.31.2.38
```

4. NAT en router LIMA
   - NAT estático para el servidor interno (172.31.2.26).

```
ip nat inside source static 172.31.2.26 209.17.220.10
```

   - NAT de sobrecarga (PAT) para la red interna (172.31.0.0 /19).

```
ip nat inside source list 20 interface FastEthernet0/0 overload
access-list 20 permit 172.31.0.0 0.0.31.255
```

   - Definiendo las entradas y la salida del servicio.

```
interface FastEthernet0/0
ip nat outside
interface FastEthernet0/1
ip nat inside
interface Serial0/0/0
ip nat inside
interface Serial0/0/1
ip nat inside
```

5. AUTENTICACIÓN EN EL ENRUTAMIENTO

- Cada router deberá configurar en sus interfaces seriales y en el enrutamiento OSPF lo siguiente:

```
interface Serial0/0/0
ip ospf message-digest-key 1 md5 7 network
!
router ospf 1
area 0 authentication message-digest
```

6. LISTAS DE CONTROL DE ACCESO

- Router Ica:

  Se tienen dos listas aplicadas a las subinterfaces, las cuales facilitan que sus Hosts de VLAN 10 puedan acceder libremente a Internet y los Host de VLAN 30, sólo a las redes internas. Al inicio de cada lista se añade una sentencia para facilitar que los mensajes broadcast de un cliente DHCP salgan libremente.

  Asimismo, estas listas de acceso evitan accesos de Telnet a los routers, el uso del protocolo ICMP entre las VLAN y hacia un router, entre otras cosas.

```
access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63

interface FastEthernet0/0.10
ip access-group 101 in

access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.255.255
access-list 103 permit ip 172.31.0.64 0.0.0.63 any

interface FastEthernet0/0.30
ip access-group 103 in
```

- Router Lima:

  Se tienen dos listas aplicadas a las subinterfaces, las cuales facilitan que sus Hosts de VLAN 30 accedan libremente a servicios web y ftp, y que los Hosts de VLAN 20 accedan sólo a las redes internas.

```
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63

interface FastEthernet0/0.10
ip access-group 102 in

access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www
access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp

interface FastEthernet0/0.30
ip access-group 103 in
```

- Router Trujillo:

  La configuración de listas es similar a la del router Ica.

```
access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.255.255
access-list 101 permit ip 172.31.1.64 0.0.0.63 any

interface FastEthernet0/0.10
ip access-group 101 in

access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63

interface FastEthernet0/0.30
ip access-group 102 in
```

DIAGNÓSTICO

- TABLA DE VECINOS

  Para el caso no se consideró establecer loopback ni router ID, por lo que cada router ha elegido a la dirección IP más alta como su router ID.

```
ICA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
209.17.220.200    0   FULL/  -        00:00:37    172.31.2.34     Serial0/0/0
```

```
LIMA#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.31.2.33       0   FULL/  -        00:00:33    172.31.2.33     Serial0/0/0
172.31.2.37       0   FULL/  -        00:00:34    172.31.2.37     Serial0/0/1
```

```
TRUJILLO#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
209.17.220.200    0   FULL/  -        00:00:33    172.31.2.38     Serial0/0/0
```

- BASE DE DATOS TOPOLÓGICA

  Obsérvese que en la lista de LINK ID aparecen los ID de cada router del área 0, así como el router que envía las rutas por defecto (tipo 5).

```
ICA#sh ip ospf database
        OSPF Router with ID (172.31.2.33) (Process ID 1)
          Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.31.2.33     172.31.2.33     1287        0x80000008 0x00fdff 5
209.17.220.200  209.17.220.200  1068        0x80000016 0x00fdff 7
172.31.2.37     172.31.2.37     1067        0x80000014 0x00fdff 6
          Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.200  841         0x80000005 0x006fd8 1
```

```
LIMA#sh ip ospf database
        OSPF Router with ID (209.17.220.200) (Process ID 1)
            Router Link States (Area 0)
Link ID       ADV Router     Age       Seq#      Checksum Link count
209.17.220.200  209.17.220.200  925       0x80000016 0x00fdff 7
172.31.2.33     172.31.2.33     1145      0x80000008 0x00fdff 5
172.31.2.37     172.31.2.37     925       0x80000014 0x00fdff 6
            Type-5 AS External Link States
Link ID       ADV Router     Age       Seq#      Checksum Tag
0.0.0.0       209.17.220.200  698       0x80000005 0x006fd8 1
```

```
TRUJILLO#sh ip ospf database
            Router Link States (Area 0)
        OSPF Router with ID (172.31.2.37) (Process ID 1)
Link ID       ADV Router     Age       Seq#      Checksum Link count
172.31.2.37     172.31.2.37     1021      0x80000014 0x00fdff 6
172.31.2.33     172.31.2.33     1242      0x80000008 0x00fdff 5
209.17.220.200  209.17.220.200  1022      0x80000016 0x00fdff 7
            Type-5 AS External Link States
Link ID       ADV Router     Age       Seq#      Checksum Tag
0.0.0.0       209.17.220.200  795       0x80000005 0x006fd8 1
```

- TABLA DE ENRUTAMIENTO

Las tablas siguientes indican la publicación, sin problemas, de las redes, considerando la autenticación.

```
ICA#SH IP ROUTE
Gateway of last resort is 172.31.2.34 to network 0.0.0.0
    172.31.0.0/16 is variably subnetted, 12 subnets, 3 masks
C       172.31.0.0/26 is directly connected, FastEthernet0/0.10
C       172.31.0.64/26 is directly connected, FastEthernet0/0.30
O       172.31.0.128/26 [110/65] via 172.31.2.34, 00:19:26, Serial0/0/0
O       172.31.0.192/26 [110/65] via 172.31.2.34, 00:19:26, Serial0/0/0
O       172.31.1.0/26 [110/129] via 172.31.2.34, 00:19:26, Serial0/0/0
O       172.31.1.64/26 [110/129] via 172.31.2.34, 00:19:26, Serial0/0/0
C       172.31.2.0/29 is directly connected, FastEthernet0/0.1
O       172.31.2.8/29 [110/65] via 172.31.2.34, 00:19:26, Serial0/0/0
O       172.31.2.16/29 [110/129] via 172.31.2.34, 00:19:26, Serial0/0/0
O       172.31.2.24/29 [110/129] via 172.31.2.34, 00:19:26, Serial0/0/0
C       172.31.2.32/30 is directly connected, Serial0/0/0
O       172.31.2.36/30 [110/128] via 172.31.2.34, 00:19:26, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.34, 00:19:26, Serial0/0/0
```

```
LIMA#SH IP ROUTE
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    172.31.0.0/16 is variably subnetted, 12 subnets, 3 masks
O       172.31.0.0/26 [110/65] via 172.31.2.33, 00:20:48, Serial0/0/0
O       172.31.0.64/26 [110/65] via 172.31.2.33, 00:20:48, Serial0/0/0
C       172.31.0.128/26 is directly connected, FastEthernet0/1.20
C       172.31.0.192/26 is directly connected, FastEthernet0/1.30
O       172.31.1.0/26 [110/65] via 172.31.2.37, 00:20:48, Serial0/0/1
O       172.31.1.64/26 [110/65] via 172.31.2.37, 00:20:48, Serial0/0/1
O       172.31.2.0/29 [110/65] via 172.31.2.33, 00:20:48, Serial0/0/0
C       172.31.2.8/29 is directly connected, FastEthernet0/1.1
```

```
O     172.31.2.16/29 [110/65] via 172.31.2.37, 00:20:48, Serial0/0/1
O     172.31.2.24/29 [110/65] via 172.31.2.37, 00:20:48, Serial0/0/1
C     172.31.2.32/30 is directly connected, Serial0/0/0
C     172.31.2.36/30 is directly connected, Serial0/0/1
C   209.17.220.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, FastEthernet0/0
```

```
TRUJILLO#SH IP ROUTE
Gateway of last resort is 172.31.2.38 to network 0.0.0.0
    172.31.0.0/16 is variably subnetted, 12 subnets, 3 masks
O     172.31.0.0/26 [110/129] via 172.31.2.38, 00:19:46, Serial0/0/0
O     172.31.0.64/26 [110/129] via 172.31.2.38, 00:19:46, Serial0/0/0
O     172.31.0.128/26 [110/65] via 172.31.2.38, 00:19:56, Serial0/0/0
O     172.31.0.192/26 [110/65] via 172.31.2.38, 00:19:56, Serial0/0/0
C     172.31.1.0/26 is directly connected, FastEthernet0/0.20
C     172.31.1.64/26 is directly connected, FastEthernet0/0.10
O     172.31.2.0/29 [110/129] via 172.31.2.38, 00:19:46, Serial0/0/0
O     172.31.2.8/29 [110/65] via 172.31.2.38, 00:19:56, Serial0/0/0
C     172.31.2.16/29 is directly connected, FastEthernet0/0.1
C     172.31.2.24/29 is directly connected, FastEthernet0/0.88
O     172.31.2.32/30 [110/128] via 172.31.2.38, 00:19:56, Serial0/0/0
C     172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.38, 00:19:56, Serial0/0/0
```

- Tabla DHCP

  Se indica que cuatro equipos reciben direcciones IP.

```
LIMA#sh ip dhcp binding
IP address      Client-ID/          Lease expiration      Type
                Hardware address
172.31.0.71     000A.F361.779B      --                    Automatic
172.31.1.6      0000.0CAA.9CDB      --                    Automatic
172.31.1.71     00D0.FF06.580C      --                    Automatic
172.31.0.6      0001.C7A9.36D0      --                    Automatic
```

- Tabla NAT

  Se comprueba la asignación estática de la dirección 209.17.220.10 hacia el servidor interno; asimismo, la traducción mediante PAT que se realiza empleando el IP de la interfaz FastEthernet 0/0.

```
LIMA#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.200:11 172.31.0.71:11     209.17.220.254:11  209.17.220.254:11
icmp 209.17.220.200:21 172.31.1.71:21     209.17.220.254:21  209.17.220.254:21
icmp 209.17.220.200:1025172.31.2.18:2     209.17.220.254:2   209.17.220.254:1025
icmp 209.17.220.200:2  172.31.2.2:2        209.17.220.254:2   209.17.220.254:2
icmp 209.17.220.10:8   172.31.2.26:8      209.17.220.254:8   209.17.220.254:8
icmp 209.17.220.200:1026172.31.2.33:2     209.17.220.254:2   209.17.220.254:1026
icmp 209.17.220.200:1024172.31.2.37:2     209.17.220.254:2   209.17.220.254:1024
---  209.17.220.10     172.31.2.26        ---                ---
```

CONFIGURACIÓN FINAL

- Router Ica:

```
ICA#sh run
Building configuration...
Current configuration : 2220 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
security passwords min-length 5
!
hostname ICA
!
login block-for 240 attempts 4 within 120
!
!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
!
aaa new-model
aaa authentication login LOCAL_AUTH local
!
!
!
!
username LIMA privilege 7 password 0 network
username uica password 0 uica
username ulima password 0 ulima
username utrujillo password 0 utrujillo
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.31.2.1 255.255.255.248
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.31.0.1 255.255.255.192
 ip helper-address 172.31.2.34
 ip access-group 101 in
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.31.0.65 255.255.255.192
 ip helper-address 172.31.2.34
 ip access-group 103 in
```

```
!
!
interface Serial0/0/0
 ip address 172.31.2.33 255.255.255.252
 ip ospf message-digest-key 1 md5 7 network
!
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 172.31.0.0 0.0.0.63 area 0
 network 172.31.0.64 0.0.0.63 area 0
 network 172.31.2.0 0.0.0.7 area 0
 network 172.31.2.32 0.0.0.7 area 0
!
ip classless
!
!
access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.255.255
access-list 103 permit ip 172.31.0.64 0.0.0.63 any
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login
 login authentication LOCAL_AUTH
line vty 0 4
 exec-timeout 5 0
 login
 login authentication LOCAL_AUTH
!
!
!
End
```

- Router Lima:

```
LIMA#sh run
Building configuration...
Current configuration : 2949 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
security passwords min-length 5
!
hostname LIMA
!
login block-for 240 attempts 4 within 120
```

```
!
!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
!
!
!
!
!
!
!
username ICA privilege 7 password 0 network
username uica password 0 uica
username ulima privilege 7 password 0 ulima
username utrujillo password 0 utrujillo
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 209.17.220.200 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 172.31.2.9 255.255.255.248
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.31.0.129 255.255.255.192
 ip access-group 102 in
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.31.0.193 255.255.255.192
 ip access-group 103 in
```

```
!
interface Serial0/0/0
 ip address 172.31.2.34 255.255.255.252
 ip ospf message-digest-key 1 md5 7 network
 ip nat inside
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.31.2.38 255.255.255.252
 ip ospf message-digest-key 1 md5 7 network
 ip nat inside
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 172.31.0.128 0.0.0.63 area 0
 network 172.31.0.192 0.0.0.63 area 0
 network 172.31.2.8 0.0.0.7 area 0
 network 172.31.2.32 0.0.0.7 area 0
 default-information originate
!
ip nat inside source list 20 interface FastEthernet0/0 overload
ip nat inside source static 172.31.2.26 209.17.220.10
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
!
access-list 20 permit 172.31.0.0 0.0.31.255
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www
access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
!
ip dhcp excluded-address 172.31.1.65 172.31.1.70
ip dhcp excluded-address 172.31.1.1 172.31.1.5
ip dhcp excluded-address 172.31.0.1 172.31.0.5
ip dhcp excluded-address 172.31.0.65 172.31.0.70
!
ip dhcp pool ica-30
 network 172.31.0.64 255.255.255.192
 default-router 172.31.0.65
ip dhcp pool t-10
 network 172.31.1.0 255.255.255.192
 default-router 172.31.1.1
ip dhcp pool t-20
 network 172.31.1.64 255.255.255.192
 default-router 172.31.1.65
ip dhcp pool ica-10
 network 172.31.0.0 255.255.255.192
 default-router 172.31.0.1
!
```

```
!
!
!
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login
 login authentication LOCAL_AUTH
line vty 0 4
 exec-timeout 5 0
 login
 login authentication LOCAL_AUTH
!
!
!
end
```

- Router Trujillo:

```
TRUJILLO#sh run
Building configuration...
Current configuration : 2265 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
security passwords min-length 5
!
hostname TRUJILLO
!
login block-for 240 attempts 4 within 120
!
!
enable secret 5 $1$mERr$h8fNeuzwQ5F8joeWZbJYw1
!
!
!
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
!
!
!
!
!
username uica privilege 15
username ulima privilege 15 password 0 ulima
username utrujillo privilege 15 password 0 utrujillo
!
!
!
!
```

```
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.31.2.17 255.255.255.248
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.31.1.65 255.255.255.192
 ip helper-address 172.31.2.38
 ip access-group 101 in
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.31.1.1 255.255.255.192
 ip helper-address 172.31.2.38
 ip access-group 102 in
!
interface FastEthernet0/0.88
 encapsulation dot1Q 88
 ip address 172.31.2.25 255.255.255.248
!
interface Serial0/0/0
 ip address 172.31.2.37 255.255.255.252
 ip ospf message-digest-key 1 md5 7 network
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 172.31.1.0 0.0.0.63 area 0
 network 172.31.1.64 0.0.0.63 area 0
 network 172.31.2.16 0.0.0.7 area 0
 network 172.31.2.36 0.0.0.3 area 0
 network 172.31.2.24 0.0.0.7 area 0
!
ip classless
!
!
access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.255.255
access-list 101 permit ip 172.31.1.64 0.0.0.63 any
!
!
!
line con 0
 exec-timeout 6 0
 logging synchronous
 login
```

```
 login authentication LOCAL_AUTH
line vty 0 4
 exec-timeout 6 0
 login
 login authentication LOCAL_AUTH
line vty 5
 exec-timeout 6 0
 login
!
!
!
end
```

- Router ISP

```
ISP#SH RUN
!
interface FastEthernet0/0
 ip address 209.17.220.254 255.255.255.0
 duplex auto
 speed auto
!
!
ip classless
ip route 172.31.0.0 255.255.224.0 209.17.220.200
!
!
!
!
```

CONCLUSIONES

_____

_____

_____

_____

TAREAS

- Modifique el encapsulamiento de los routers hacia Internet con PPP mediante CHAP.
- Establezca las VLAN en un dominio VTP.
- Modifique el enrutamiento OSPF a EIGRP en el enlace Lima – Trujillo.

LABORATORIO N° 9 - Principios básicos de conmutación y enrutamiento intermedio

INTRODUCCIÓN

El presente trabajo está desarrollado con la finalidad de describir y demostrar los principios básicos de conmutación y enrutamiento intermedio, para lo cual se plantea un caso a través de una serie de requisitos tanto teóricos como prácticos, en que se aplican estrategias de escalabilidad, métodos de configuración, compatibilidad y seguridad de la red. Tiene por finalidad la implementación de una red empresarial.

OBJETIVO

- Implementar un esquema de solución de red de acuerdo a los principios de enrutamiento y conmutación.

DESCRIPCIÓN GENERAL

El siguiente estudio de caso se utiliza para ilustrar el proceso y la documentación que se requieren para el diseño de una red. Este estudio de caso presenta un escenario en el que la empresa Investigación ABC ha contratado a un grupo consultor de red para diseñar su red.

Para organizar este proyecto, el escenario se ha dividido en seis fases, cada una de las cuales presenta sus requisitos. Se ha completado una planilla de trabajo para cada una de las partes.

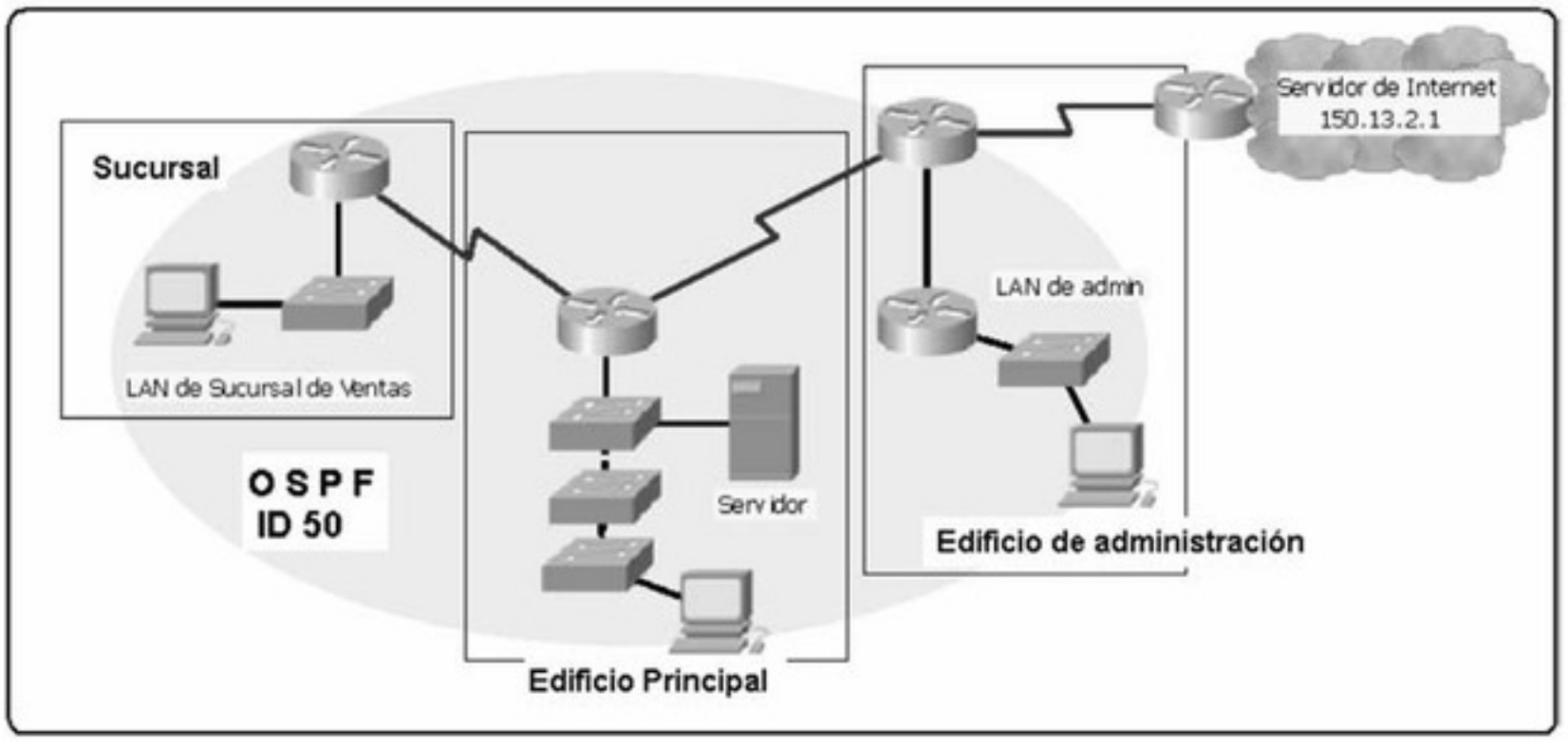
Se ha preparado un informe formal, similar al que se entregará a la empresa una vez que se hayan completado todas las tareas.

Se requiere de la realización de las siguientes actividades:

- Usar los recursos suministrados, el diagrama y la narrativa, para configurar la red física.
- Configurar un esquema de división en subredes utilizando VLSM.
- Configurar los routers según sea necesario.
- Establecer y configurar los switches y las VLAN, según sea necesario.
- Verificar y realizar el diagnóstico de fallas de todas las conexiones.
- Suministrar documentación detallada en el formato adecuado.
- Suministrar un informe final por escrito.

Escenario

La empresa Investigación ABC es una pequeña empresa que desarrolla productos inalámbricos de alta velocidad. La oficina principal ocupa dos edificios en Sydney. Uno de los edificios corresponde al Grupo de Administración. El otro edificio está destinado al Grupo de Ventas y Mercadeo, y al Grupo de Investigación y Desarrollo, que es más grande. Los empleados del Grupo de Investigación, y del Grupo de Ventas y Mercadeo estarán distribuidos en los tres pisos del edificio principal. La empresa Investigación ABC también posee una sucursal de ventas en Melbourne.



DESARROLLO

El proyecto se ha documentado en tres partes:

I. **Descripción de fases**

Se indica la configuración VLSM, las diferencias y ventajas del protocolo OSPF, la configuración aplicada en las VLAN, y la configuración ejecutada en los routers y switches, amén de otras configuraciones.

II. **Diagramas físicos y lógicos de la red empresarial**

Se muestra de manera gráfica la distribución de equipos en la red, la denominación que se le ha dado a cada enlace y las interfaces empleadas en cada dispositivo; asimismo, la distribución de direcciones en cada equipo.

III. **Resultados de la configuración de routers**

Se presentan los resultados obtenidos con los comandos de prueba en la red, para los routers y switches que se han empleado.

I. DESCRIPCIÓN DE FASES

FASE 1: Requisitos

La empresa ha entregado un diagrama lógico de la red.

Requisitos de la empresa Investigación ABC:

- 20 empleados en el Grupo de Investigación y Desarrollo.
- 10 empleados en el Grupo de Ventas y Mercadeo.
- 7 empleados en el Grupo de Administración.
  - 2 empleados en la oficina de ventas remota.
  - Vida útil máxima de 5 servidores en una subred separada, más allá del crecimiento de la empresa.
  - Usar la subred 200.200.100.0/30 para conectarse al router de Internet.
  - Usar la red pública Clase C 225.0.0.0 para el direccionamiento interno.
  - Usar VLSM para el direccionamiento IP.

- Esperar un crecimiento del 100% de los requisitos IP al determinar el tamaño de las subredes.
- Todos los dispositivos de networking deben tener direcciones IP.
- Servidor HTTP con dirección 225.0.0.33/27.

Desarrollo del direccionamiento con VLSM:

- Aplicando el sistema de direccionamiento mediante VLSM para configurar el esquema de división en subredes:
- Se empieza por la(s) subred(es) más grande(s) y luego se va(n) subdividiendo, tratando de completar las subredes hasta los rangos permisibles de Host (2, 6, 14, 30, 62, etc.)

1. En este caso el área de **Investigación y Desarrollo** es la mayor y requiere de una subred de 40 Hosts (20 + 100%). Se deberán establecer 62 (64-2) direcciones IP para toda la subred, ya que es el rango más adecuado.
   - De lo anterior se deduce que la red empresarial se ha subdivido en cuatro subredes de 64 IP cada una.
   - Hay que tener en cuenta que se podrá usar cualquiera de las cuatro subredes para cubrir el requerimiento.
2. La red empresarial tiene cuatro subredes de 64 direcciones IP cada una. Se requiere ahora de una subdivisión menor para:
   - El área de **Ventas y Mercadeo**, 20 Hosts (10 + 100%); el rango más cercano sería de 30 Hosts.
   - El área de **servidores**. Se exige la dirección IP del servidor HTTP 225.0.0.33/27, lo que equivale a 30 Hosts.

   Para cubrir esta necesidad se toma una de las subredes de 64 direcciones.
3. Seguidamente quedan dos subredes de 64 direcciones IP. Con lo que se continúa la subdivisión; en este caso una subred quedará sin usar y la otra se subdividirá como sigue:
   - **Grupo de Lan administrativa**, con 14 Hosts (7 + 100%); el rango más cercano coincide con el de 14 Hosts, (16-2) direcciones IP.
   - La **oficina remota** requiere de 12 Hosts (6 +100%); el rango más cercano sería de 14 Hosts, (16-2) direcciones IP.
   - Enlace entre el **router de salida de VLAN y los switches**. Se requiere de 4 Hosts; el rango más cercano sería de 6 Hosts, (8-2) direcciones IP.
   - Enlace entre el **router 1** y el **router 2**; el rango más cercano coincide con el de 2 Hosts, (4-2) direcciones IP.
   - Enlace entre el **router 1** y el **router 3**; el rango más cercano coincide con el de 2 Hosts, (4-2) direcciones IP.
   - Enlace entre el **router 3** y el **router 4**; el rango más cercano coincide con el de 2 Hosts, (4-2) direcciones IP.

   De la subred dividida se utilizarán 52 direcciones divididas en seis subredes, quedando 12 direcciones sin usar (para dos subredes de ocho y cuatro, o tres subredes de cuatro cada una).

Planilla de trabajo

1. Se ha utilizado el diseño VLSM para maximizar el uso de direcciones IP. Se ha creado una tabla en la que figuran todas las subredes posibles que satisfacen los requisitos de la empresa, utilizando un diseño VLSM. Las subredes que no se utilizarán están identificadas en la tabla.

   A continuación se suministra un diagrama de tabla de muestra que se usa para registrar el diseño VLSM.

Cantidad de direcciones de Host requeridas	Dirección de red	Máscara de subred	Cantidad máxima de Hosts posible	En uso (sí / no)	Nombre de la red
--------	225.0.0.0 /27	255.255.255.224	30	No	----------
5→10	225.0.0.32 /27	255.255.255.224	30	Sí	Servidores
20 →40	225.0.0.64 /26	255.255.255.192	62	Sí	Investigación y Desarrollo
7→14	225.0.0.128 /28	255.255.255.240	14	Sí	Grupo de Administración
6 →12	225.0.0.144 /28	255.255.255.240	14	Sí	Oficina remota
2	225.0.0.160 /30	255.255.255.252	2	Sí	Enlace R1 y R2
2	225.0.0.164 /30	255.255.255.252	2	Sí	Enlace R1 y R3
2	225.0.0.168 /30	255.255.255.252	2	Sí	Enlace R3 y R4
--------	225.0.0.172 /29	255.255.255.224	2	No	----------
--------	225.0.0.176 /28	255.255.255.224	14	No	----------
10→20	225.0.0.192 /27	255.255.255.224	30	Sí	Ventas y Mercadeo
--------	225.0.0.224 /27	255.255.255.224	30	No	----------

2. Para cada ubicación, incluyendo Internet, se presentan estas tablas que sirven de ayuda para las actividades de diseño y desarrollo, y se usan al configurar switches y routers.

   A continuación se suministra un esquema de muestra para los routers.

Ubicación: Enlace con ISP
Nombre del router: Router-1

Tipo / número de interfaz /	Descripción y objetivo	DCE /DTE (si corresponde)	Velocidad de reloj	Nombre de la red	Número de la red	Dirección de IP de la interfaz	Máscara de subred
Serial 0	Acceso a Internet	DCE	64000	Internet	200.200.100.0	200.200.100.2	255.255.255.252
FastEthernet 0/0	Acceso a Lan administrativa	--------	---------	Enlace a Lan administrativa	225.0.0.160	225.0.0.161	255.255.255.252
Serial 1	Acceso a las VLAN y Lan remota	DTE		Enlace principal a red empresarial	225.0.0.164	225.0.0.165	255.255.255.252
Loopback 0	ID de router OSPF	---------	---------	---------	---------	192.168.1.1	255.255.255.255

Ubicación: Enlace con Router-1 y Lan administrativa
Nombre del router: Router-2

Tipo / número de interfaz / subinterfaz	Descripción y objetivo	DCE /DTE (si corresponde)	Velocidad de reloj	Nombre de la red	Número de la red	Dirección de IP de la interfaz	Máscara de subred
FastEthernet 0/0	Acceso a la red empresarial e Internet	--------	---------	Enlace a Lan administrativa	225.0.0.160	225.0.0.162	255.255.255.252
FastEthernet 0/1	Acceso a Lan administrativa	--------	---------	Lan administrativa	225.0.0.128	225.0.0.129	255.255.255.240
Loopback 0	ID de router OSPF	---------	---------	---------	---------	192.168.1.22	255.255.255.255

Ubicación: Enlace de las VLAN con toda la red (puerta de enlace), hacia el Router-1 y Router-4 (Lan remota)
Nombre del router: Router-3

Tipo / número de interfaz / subinterfaz	Descripción y objetivo	DCE /DTE (si corresponde)	Velocidad de reloj	Nombre de la red	Número de la red	Dirección de IP de la interfaz	Máscara de subred
Serial 0	Acceso a Lan remota	DTE	-----	Enlace a Lan remota	225.0.0.168	225.0.0.169	255.255.255.252
Serial 1	Acceso a Lan administrativa e Internet	DCE	64000	Enlace principal a red empresarial	225.0.0.164	225.0.0.166	255.255.255.252
FastEthernet 0/0.1	Acceso a VLAN 2	--------	---------	Investigación	225.0.0.192	225.0.0.193	255.255.255.192
FastEthernet 0/0.2	Acceso a VLAN 3	--------	---------	Ventas y Mercadeo	225.0.0.32	225.0.0.62	255.255.255.224
FastEthernet 0/0.3	Acceso a VLAN 4	--------	---------	Servidores	225.0.0.64	225.0.0.65	255.255.255.224
Loopback 0	ID de router OSPF	---------	---------	---------	---------	192.168.1.3	255.255.255.255

Ubicación: Lan remota, enlace hacia Router-3

Nombre del router: Router-4

Tipo / número de interfaz	Descripción y objetivo	DCE /DTE (si corresponde)	Velocidad de reloj	Nombre de la red	Número de la red	Dirección de IP de la interfaz	Máscara de subred
Serial 0	Acceso a Lan Remota	DCE	64000	Enlace a Lan remota	225.0.0.168	225.0.0.170	255.255.255.252
FastEthernet 0/0	Lan remota	----------	--------	Lan remota	225.0.0.144	225.0.0.145	255.255.255.240
Loopback 0	ID de router OSPF	---------	---------	---------	---------	192.168.1.4	255.255.255.255

Ubicación: Enlace con Router-1

Nombre del router: ISP

Tipo / número de interfaz	Descripción y objetivo	DCE /DTE (si corresponde)	Velocidad de reloj	Nombre de la red	Número de la red	Dirección de IP de la interfaz	Máscara de subred
Serial 0	Acceso a Internet	DTE	----------	Internet	200.200.100.0	200.200.100.1	255.255.255.252
Loopback 0	ID de router OSPF	---------	---------	---------	---------	150.13.2.1	255.255.255.255

TABLAS DE SWITCH

Ubicación: Piso 1

Nombre del switch: Sw-1

Dirección IP del switch:

Tipo / puerto	Descripción	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
0/5, 0/6, 0/7. 0/8. 0/9. 0/10, 0/11	VLAN administrativa	100 mbps	full	Administrativa	----------	----------	1	Fast ethernet	----------
0/3	VLAN 10	100 mbps	full	Investigación	225.0.0.64	255.255.255.192	10	Fast ethernet	----------
0/4	VLAN 20	100 mbps	full	Ventas y Mercadeo	225.0.0.192	255.255.255.224	20	Fast ethernet	----------
0/2	VLAN 30	100 mbps	full	Servers	225.0.0.32	255.255.255.224	30	Fast ethernet	----------
0/1	Enlace troncal al router	100 mbps	full	----------	----------	----------	------	Fast ethernet	Dot1q
0/12	Enlace troncal al Sw-2	100 mbps	full	----------	----------	----------	------	Fast ethernet	Dot1q

Ubicación: Piso 2

Nombre del switch: Sw-2

Dirección IP del switch:

Tipo / puerto	Descripción	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
0/1, 0/2, 0/5, 0/6, 0/7, 0/8, 0/9y 0/10	VLAN administrativa	100 mbps	full	Administrativa	----------	----------	1	Fast ethernet	----------
0/3	VLAN 10	100 mbps	full	Investigación	225.0.0.64	255.255.255.192	10	Fast ethernet	----------
0/4	VLAN 20	100 mbps	full	Ventas y Mercadeo	225.0.0.192	255.255.255.224	20	Fast ethernet	----------
0/11	Enlace trocal al Sw-3	100 mbps	full	----------	----------	----------	------	Fast ethernet	Dot1q
0/12	Enlace trocal al Sw-1	100 mbps	full	----------	----------	----------	------	Fast ethernet	Dot1q

Ubicación: Piso 3

Nombre del switch: Sw-3

Dirección IP del switch:

Tipo / puerto	Descripción	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
0/1, 0/2, 0/5, 0/6, 0/7. 0/8. 0/9. 0/10, 0/11	VLAN administrativa	100 mbps	full	Administrativa	----------	----------	1	Fast ethernet	----------
0/3,	VLAN 10	100 mbps	full	Investigación	225.0.0.	255.255.255.192	10	Fast ethernet	----------
0/4	VLAN 20	100 mbps	full	Ventas y Mercadeo	225.0.0.	255.255.255.224	20	Fast ethernet	----------
0/12	Enlace troncal al Sw-2	100 mbps	full	----------	----------	----------	------	Fast ethernet	Dot1q

3. Asignación y tabulación de las direcciones de la PC/estación de trabajo y del servidor, para cada Lan en cada ubicación. El servidor HTTP será 225.0.0.33/27.

Nombre de la Lan	Nombre de la PC o servidor	Dirección IP	Máscara de subred	Gateway	Servicios suministrados
VLAN 10 Investigación	PC1-10	225.0.0.66	255.255.255.192	225.0.0.65	Punto de acceso a la VLAN 10 y red empresarial
	PC2-10	225.0.0.67	255.255.255.192	225.0.0.65	Punto de acceso a la VLAN 10 y red empresarial
	PC3-10	225.0.0.68	255.255.255.192	225.0.0.65	Punto de acceso a la VLAN 10 y red empresarial
VLAN 20 Ventas y Mercadeo	PC1-20	225.0.0.194	255.255.255.224	225.0.0.193	Punto de acceso a la VLAN 20 y red empresarial
	PC2-20	225.0.0.195	255.255.255.224	225.0.0.193	Punto de acceso a la VLAN 20 y red empresarial
	PC3-20	225.0.0.196	255.255.255.224	225.0.0.193	Punto de acceso a la VLAN 20 y red empresarial
VLAN 30 Servers	HTTP	225.0.0.33	255.255.255.224	225.0.0.62	Servicio DHCP y web
Lan remota	PC-remota	225.0.0.146	255.255.255.240	225.0.0.145	Punto de acceso remoto a la red empresarial
Lan administrativa	PC-admin	225.0.0.130	255.255.255.240	225.0.0.129	Punto de acceso administrativo a la red empresarial

Fase 2: Protocolos de enrutamiento

Se le recomienda un protocolo de enrutamiento para la red.

Planilla de trabajo

Las alternativas y propiedades de los posibles protocolos de enrutamiento se han identificado, para definir su uso, con un número entre 0 y 3.

Los valores son establecidos de acuerdo al nivel de facilidad para trabajar con una propiedad, como sigue: 0 = malo, 1 = regular, 2 = bueno y 3 = excelente.

Protocolo	PROPIEDADES						Total
	VLSM	Facilidad de configuración	Elección de rutas (Métrica = M)	Tipo de protocolo	Prevención de bucles	Escalabilidad	
OSPF	Sí	No, se requiere de un administrador experimentado	Velocidad del enlace (elección de la ruta más libre y más corta)	ESTADO DE ENLACE Publican los estados de sus enlaces desde la perspectiva de sus vecinos (LSA)	En las redes de broadcast, el intervalo hello, por defecto, es de 10 segundos y en las que no son, es de 30 segundos	Apropiado para internet works grandes y escalables	18
RIP V1	No	Sí	Número de saltos (elección de rutas lentas)	VECTOR-DISTANCIA Aprenden rutas y luego las envían a los vecinos directamente conectados	• Temporizadores de espera • Horizonte dividido	Para pequeñas redes y la mejor ruta se basa en el menor número de saltos	10
RIP V2	Sí	Sí	Número de saltos (elección de rutas lentas)		• Temporizadores de espera • Horizonte dividido		14
IGRP	No	Sí	Número de saltos máximo de 255. 7 M = 10/BW		• Lapsos de espera • Horizontes divididos • Actualizaciones inversas envenenadas	No tiene compatibilidad multiprotocolo	14
EIGRP	Sí	Sí	El límite máximo para el número de saltos es 224. 7 M = 10/BW * 256	Protocolo vector distancia avanzado y actúa como estado de enlace al actualizar los vecinos y mantener la información de enrutamiento	Tiempos de convergencia más rápidos y gestión superior de los bucles de enrutamiento	Con compatibilidad multiprotocolo, mejor escalabilidad por el número de saltos	16

Recomendación del grupo para el protocolo de enrutamiento: **OSPF**, por el nivel de funcionalidad según las exigencias solicitadas**.**

Fase 3: OSPF

Se ha decidido utilizar OSPF como protocolo de enrutamiento.

Requisitos de la empresa Investigación ABC

ID 50 del proceso OSPF.

Todos los routers en una sola área: el área 0.

Dirección de loopback asignada en cada router.

Dirección de loopback utilizada como ID del router OSPF.

Hay una red de acceso múltiple en el edificio de Administración y se debe elegir un DR.

Determinar si se debe usar la ID del router o la prioridad de interfaz para determinar el DR en el edificio de Administración.

Planilla de trabajo

1. A continuación se explican las razones por las que se ha elegido la ID de router o prioridad de interfaz para determinar el DR:

   En las redes multiacceso con OSPF, el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR).

   El DR será el punto de enfoque de todas las actualizaciones del estado de enlace y de las publicaciones del estado de enlace. Debido a que la función del DR es crítica, se elige un router designado de respaldo (BDR) para que reemplace al DR en caso de que éste falle.

   Si el tipo de red de una interfaz es broadcast, la prioridad OSPF por defecto es 1 (se pueden establecer entre 0 a 255). Cuando las prioridades OSPF son iguales, la elección de OSPF para DR se decide sobre la base del ID del router (dirección IP asignada a una interfaz o dirección loopback).

   Si no existe ninguna interfaz activa, el proceso OSPF no se iniciará. Para asegurar la estabilidad de OSPF, deberá haber una interfaz activa para el proceso OSPF en todo momento. Es posible configurar una interfaz de loopback, que es una interfaz lógica, para este propósito.

En principio, al tratar de definir al Router-2 como DR se verificaron las características de su dirección IP en sus puertos de interfaz FastEthernet 0/0 y 0/1; luego, su dirección de loopback y finalmente se vio la facilidad para modificar la prioridad en la interfaz FastEthernet de ambos routers.

2. Explique las razones por las que ha elegido el Router-2 como DR en el edificio de Administración.

   Por cuestiones de facilidad en la administración se definió a dicho router como el DR, ya que está más cerca de la Lan administrativa.

3. ¿Es necesario establecer un DR en las conexiones seriales entre los edificios y la sucursal remota? No.

   ¿Por qué? Porque en un enlace serial punto a punto no se necesita establecer el DR ni el BDR.

Fase 4: VLAN

La empresa ahora desea obtener información acerca de las VLAN. Éstas son necesarias para el edificio principal. La empresa ha brindado la siguiente información:

Requisitos de la empresa Investigación ABC

- Hay 20 empleados del Grupo de Investigación y Desarrollo.
- Hay 9 empleados del Grupo de Ventas y Mercadeo.
- 8 miembros del personal de Investigación y 2 miembros del personal de Ventas están en el piso 3.
- 8 miembros del personal de Investigación y 4 miembros del personal de Ventas están en el piso 2.
- 4 miembros del personal de Investigación y 3 miembros del personal de Ventas están en el piso 1.
- En el piso 1 se encuentra también la Lan del servidor. Hay cinco máquinas con capacidad de servidor pero por el momento sólo hay una disponible.
- Hay habitaciones separadas en cada piso para los grupos de trabajo.
- Hay suficiente espacio en cada habitación para adaptarse al crecimiento.
- El 100% del crecimiento pronosticado se producirá de modo uniforme por piso.
- Los switches del edificio principal están conectados en forma de loop, de modo que si un switch falla, se utilizará una ruta alternativa.
- Hay un switch por piso que comparten las distintas subredes.
- La raíz del spanning tree se debe ubicar en una posición óptima.

Área o grupo	Requerimientos actuales	Distribución por piso	+ el 100% del crecimiento	
Investigación y Desarrollo	18 empleados	8 en el piso 3	36 Hosts	16 en el piso 3
		6 en el piso 2		12 en el piso 2.
		4 en el piso 1		8 en el piso 1
Ventas y Mercadeo	9 empleados	2 en el piso 3	18 Hosts	4 en el piso 3
		4 en el piso 2.		8 en el piso 2
		3 en el piso 1		6 en el piso 1
Lan del servidor	5 equipos servidores	5 en el piso 1	5	

Planilla de trabajo

1. Se muestran tablas que documentan las asignaciones de puertos VLAN del switch para el equipo de demostración disponible.

   Detalles del switch

Nombre de switch	Modelo	Nº de puertos	Ubicación	Dirección IP	Gateway	VLAN de administración	Modo VTP	Dominio VTP	Raíz STP
Sw -1	Catalyst 2950	12	Piso 1	----------	----------	VLAN 1	Server	Dominio ABC	Switch designado
Sw -2	Catalyst 2950	12	Piso 2	----------	----------	VLAN 1	Client	Dominio ABC	Root bridge
Sw -3	Catalyst 2950	12	Piso 3	----------	----------	VLAN 1	Client	Dominio ABC	Switch designado

2. A continuación se describe la decisión tomada sobre el puente raíz STP.

   Los puentes y switches Ethernet pueden implementar el protocolo spanning tree IEEE 802.1d y usar el algoritmo spanning tree para desarrollar una red de ruta más corta, sin loops. La ruta más corta se basa en costos de enlace acumulativos. Los costos de enlace se basan en la velocidad del enlace.

   El protocolo spanning tree establece un nodo raíz denominado puente raíz. El protocolo spanning tree desarrolla una topología que tiene una ruta para llegar a todos los nodos de la red. El árbol se origina desde el puente raíz. En los enlaces redundantes que no forman parte del árbol, la ruta más corta se bloquea.

   Cuando el switch se enciende, se usa el algoritmo spanning tree para identificar el puente raíz. Las BPDU son enviadas con el ID de puente (BID). El BID se compone de una prioridad de puente que asume un valor por defecto de 32768 y la dirección MAC del switch.

   El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto, lo que hace que el BID sea más pequeño.

Fase 5: Verificar la red

Demostración de la funcionalidad de la red del edificio principal e instalación de una red lógica equivalente con el equipo suministrado.

Se instaló una máquina como servidor HTTP en la VLAN del servidor y un Host cliente en cada una de las otras VLAN.

Comprobar que todos los dispositivos estén configurados.

Todas las configuraciones, tablas de enrutamiento y bases de datos de VLAN están registradas como parte de la documentación.

Estrategia de prueba y verificación

1. Demostrando el enrutamiento entre las VLAN del edificio principal:
   - La prueba se realizó con el comando PING desde las diferentes VLAN, donde se emitió una respuesta desde el Host destino.

Desde VLAN / SW	A VLAN / SW	PROTOCOLO	HOST	APROBADO / RECHAZADO
PC1-10 (sw-1)	20 (sw-1)	ICMP / VTP	PC-1-20	Aprobado
PC3-10 (sw-3)	20 (sw-2)	ICMP / VTP	PC-2-20	Aprobado
PC2-10 (sw-1)	20 (sw-3)	ICMP / VTP	PC-3-20	Aprobado
PC1-10 (sw-1)	30 (sw-1)	ICMP / VTP	HTTP	Aprobado
HTTP (sw-1)	20 (sw-1)	ICMP / VTP	PC-1-20	Aprobado
VLAN 1 (sw-1)	10 (sw-2)	ICMP / VTP	PC-2-10	Aprobado
VLAN 1 (sw-2)	20 (sw-3)	ICMP / VTP	PC-3-20	Aprobado
VLAN 1 (sw-3)	30 (sw-1)	ICMP / VTP	HTTP	Aprobado

2. Demostrando el acceso de todos los Hosts entre sí y el servicio HTTP en la máquina del servidor.
   - La prueba se realizó con el comando PING, donde se emitió una respuesta desde el Host destino.

Desde el Host	Al Host	Aprobado / rechazado
PC1-10	PC2-10	Aprobado
PC1-10	PC3-10	Aprobado
PC1-10	PC1-20	Aprobado
PC1-10	PC2-20	Aprobado
PC1-10	PC3-20	Aprobado
PC1-10	HTTP	Aprobado
PC2-10	PC3-10	Aprobado

Desde el Host	Al Host	Aprobado / rechazado
PC2-10	PC1-20	Aprobado
PC2-10	PC2-20	Aprobado
PC2-10	PC3-20	Aprobado
PC2-10	HTTP	Aprobado
PC3-10	PC1-20	Aprobado
PC3-10	PC2-20	Aprobado
PC3-10	PC3-20	Aprobado

Desde el Host	Al Host	Aprobado / rechazado
PC3-10	HTTP	Aprobado
PC1-20	PC2-20	Aprobado
PC1-20	PC3-20	Aprobado
PC1-20	HTTP	Aprobado
PC2-20	PC3-20	Aprobado
PC2-20	HTTP	Aprobado
PC3-20	HTTP	Aprobado

3. Comportamiento de Internet work cuando falla un solo enlace troncal.

Desde el Host	Al Host	Enlace troncal arriba / abajo	Ruta	Aprobado / rechazado
PC1-10	PC2-10	Enlace troncal entre Sw-1 (puerto 12) y Sw-2 (puerto 11)	Sw-1, Sw-3 y Sw-2	Aprobado
PC2-10	PC3-10	Enlace troncal entre Sw-2 (puerto 12) y Sw-3 (puerto 12)	Sw-2, Sw-1 y Sw-3	Aprobado
PC1-10	PC2-20	Enlace troncal entre Sw-1 (puerto 12) y Sw-2 (puerto 11)	Sw-1, Router-3, Sw-1, Sw-3 y Sw-2	Aprobado
PC2-20	HTTP	Enlace troncal entre Sw-2 (puerto 12) y Sw-3 (puerto 12)	Sw-2, Sw-1 y Sw-3	Aprobado
HTTP	PC3-10	Enlace troncal entre Sw-1 (puerto 12) y Sw-2 (puerto 11)	Sw-1, Sw-3 y Sw-2	Aprobado

Fase 6: Demostración final

Demostración de Internet work completo.

- Se han configurado todos los dispositivos y se muestra el acceso a la dirección del servidor de Internet desde todas las redes.

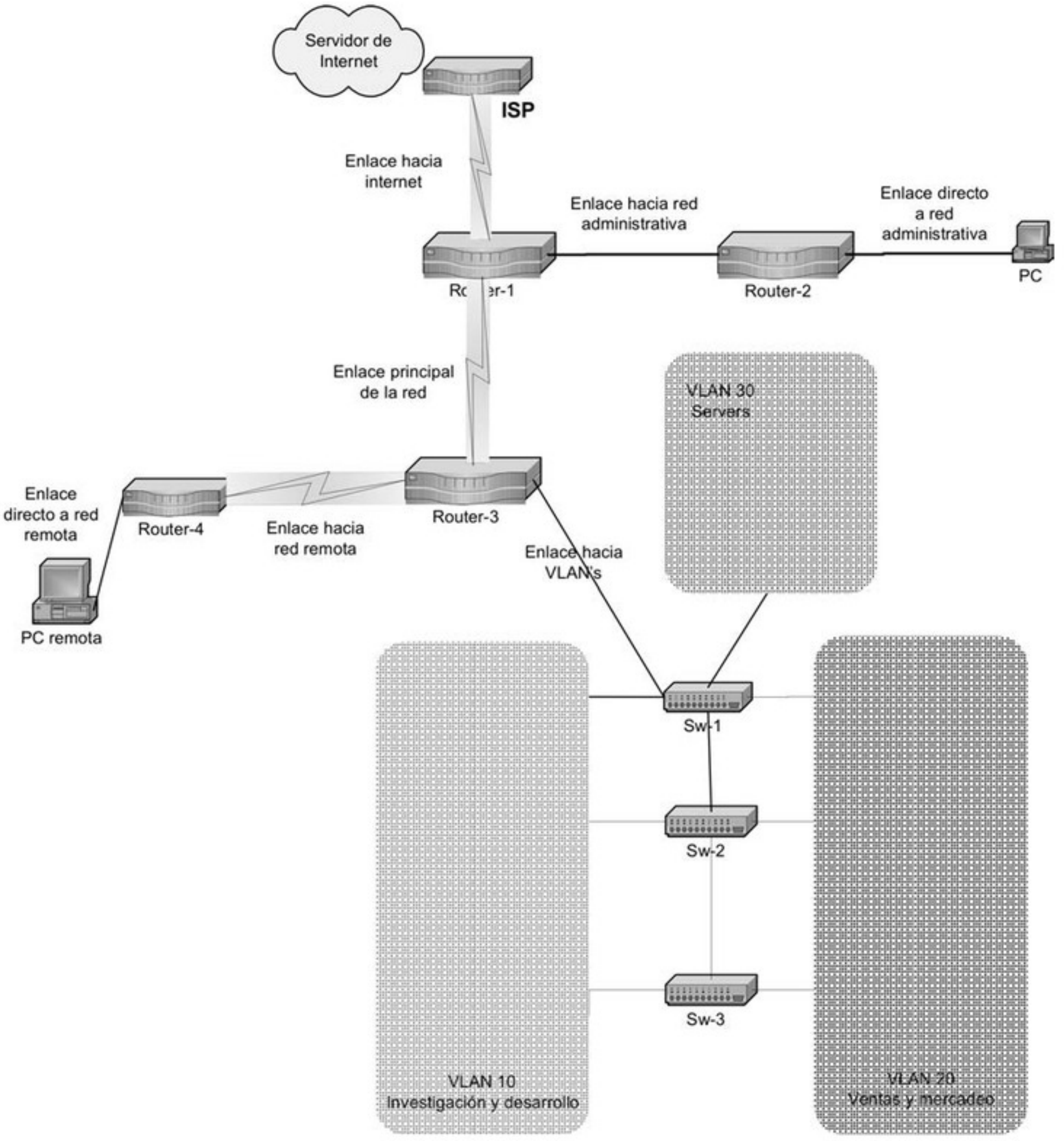
Resultados resumidos de la prueba:

Desde el Host		Al Host	Ruta que se ha verificado	Ruta que se ha tomado	Aprobado / rechazado
VLAN 10	PC1-10	PC2-10	Conectividad por enlaces troncales para la VLAN 10	Sw-1 y Sw-2	Aprobado
	PC2-10	PC3-10	Conectividad por enlaces troncales para la VLAN 10	Sw-2 y Sw-3	Aprobado
	PC3-10	PC1-10	Conectividad por enlaces troncales para la VLAN 10	Sw-3, Sw-2 y Sw-1	Aprobado
PC3-10		PC2-10	Enrutamiento entre VLAN 10 y 20, con enlaces troncales	Sw-3, Sw-2, Sw-1, router-3, Sw-1 y Sw-2	Aprobado
VLAN 20	PC1-20	PC2-20	Conectividad por enlaces troncales para la VLAN 20	Sw-1 y Sw-2	Aprobado
	PC2-20	PC3-20	Conectividad por enlaces troncales para la VLAN 20	Sw-2 y Sw-3	Aprobado
	PC3-20	PC1-20	Conectividad por enlaces troncales para la VLAN 20	Sw-3, Sw-2 y Sw-1	Aprobado
HTTP		PC1-10 (VLAN 10)	Enrutamiento entre VLAN 30 y 10, con enlaces troncales	Sw-1, Router-3 y Sw-1	Aprobado
HTTP		PC1-20 (VLAN 20)	Enrutamiento entre VLAN 30 y 20, con enlaces troncales	Sw-1, Router-3, Sw-1 y Sw-2	Aprobado
HTTP		PC-remota	Enrutamiento de VLAN 30 hacia la Lan remota	Sw-1, Router-3 y Router-4	Aprobado
PC-remota		PC2-10 (VLAN 10)	Enrutamiento desde la Lan remota hacia la VLAN 30	Router-4, Router-3, Sw-1 y Sw-2	Aprobado
PC-remota		PC3-30 (VLAN 20)	Enrutamiento desde la Lan remota hacia la VLAN 20	Router-4, Router-3, Sw-1, Sw-2 y Sw-3	Aprobado
PC-remota		PC-admin	Enrutamiento desde la Lan remota hacia la Lan administ.	Router-4, Router-3, Router-1 y Router-2	Aprobado
PC-admin		PC3-10 (VLAN 10)	Enrutamiento desde la Lan administrativa hacia VLAN 10	Router-2, Router-1, Router-3, Sw-1, Sw-2 y Sw-3	Aprobado
PC-admin		PC2-20 (VLAN 20)	Enrutamiento desde la Lan administrativa hacia VLAN 20	Router-2, Router-1, Router-3, Sw-1 y Sw-2	Aprobado
PC-admin		HTTP	Enrutamiento desde la Lan administrativa hacia VLAN 30	Router-2, Router-1, Router-3 y Sw-1	Aprobado
PC2-10		Internet	Enrutamiento desde la VLAN 10 hacia Internet	Sw-2, Sw-1, Router-3, Router-1 e ISP	Aprobado
PC1-20		Internet	Enrutamiento desde la VLAN 20 hacia Internet	Sw-1, Router-3, Router-1 e ISP	Aprobado
HTTP		Internet	Enrutamiento desde la VLAN 30 hacia Internet	Sw-1, Router-3, Router-1 e ISP	Aprobado
PC-remota		Internet	Enrutamiento desde la Lan remota hacia Internet	Router-4, Router-3, Router-1 e ISP	Aprobado
PC-admin		Internet	Enrutamiento desde la Lan administrativa hacia internet	Router-2, Router-1 e ISP	Aprobado

II. DIAGRAMAS FÍSICOS Y LÓGICOS DE LA RED EMPRESARIAL

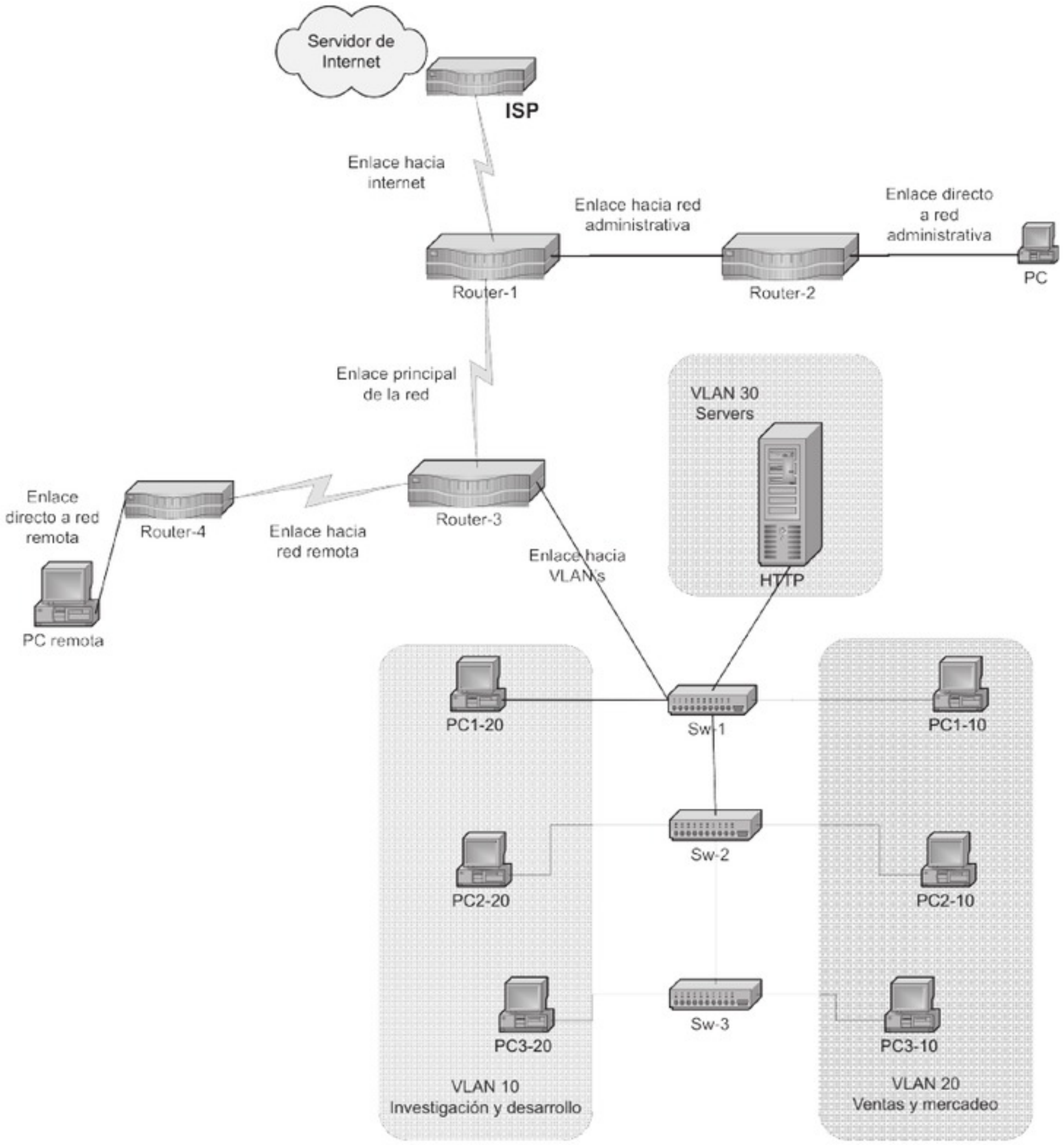
1. DIAGRAMA FÍSICO:

Se indican a continuación la denominación de cada red y la distribución física de los equipos:



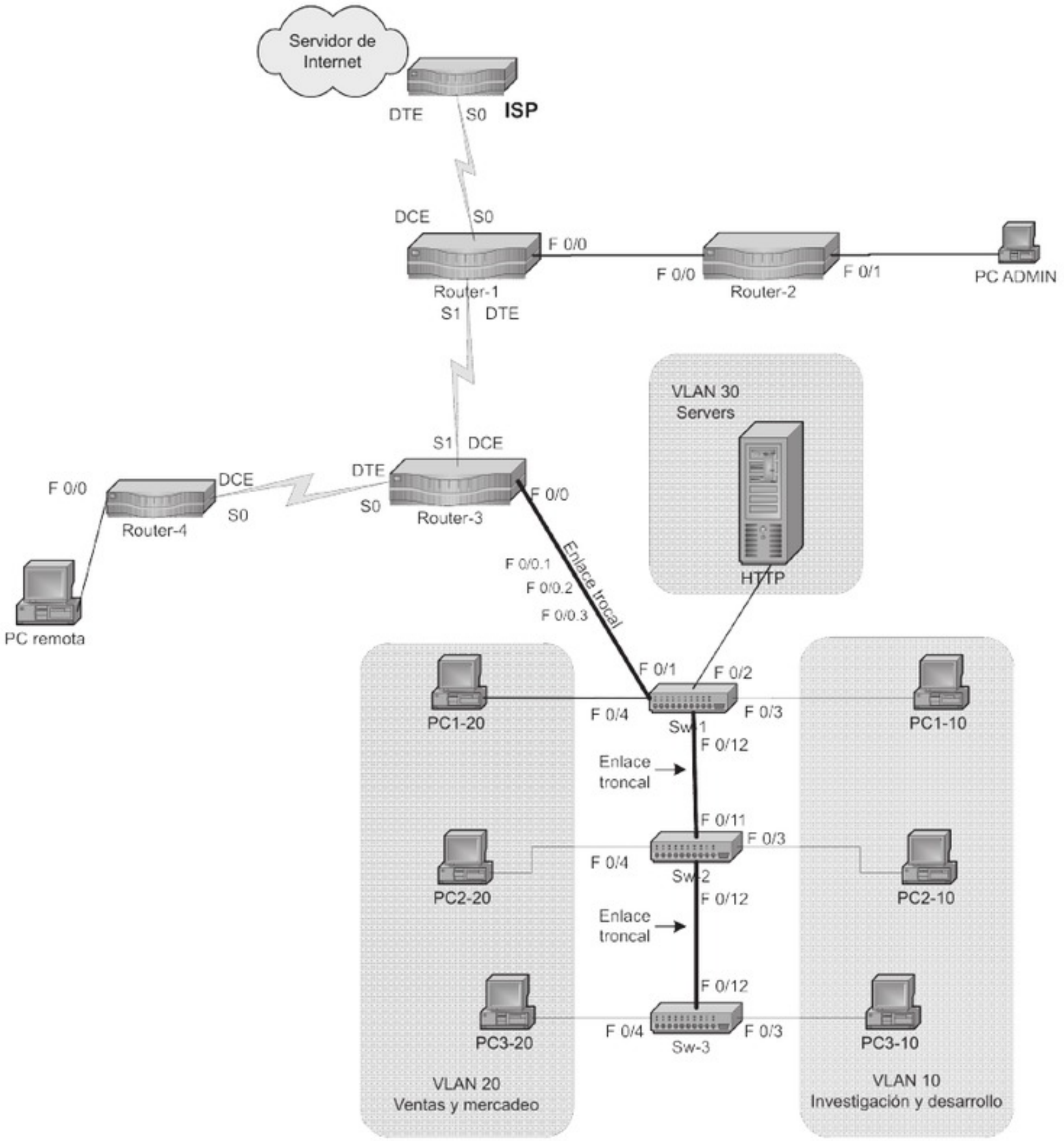
2. **DIAGRAMA LÓGICO:**

Se indica la denominación de los equipos y las interfaces empleadas para su configuración; asimismo, las características de cómo trabajarán algunas interfaces.



3. **DIAGRAMA LÓGICO**:

Se indican las direcciones lógicas empleadas para cada puerto de interfaz.



III. RESULTADOS DE LA CONFIGURACIÓN DE ROUTERS:

1. DIAGNÓSTICO DE VECINOS

```
Router-1#sh cdp neighbors
……<resultado omitido>……
Device ID      Local Intrfce    Holdtme   Capability  Platform  Port ID
Switch1900       Fas0        165        T S     1912     1
Router-3         Ser1        175        R       2620     2
ISP              Ser0        180        R       2620     1

Router-2#sh cdp neighbors
……<resultado omitido>……
Device ID      Local Intrfce    Holdtme   Capability  Platform  Port ID
Switch1900       Fas0        169        T S     1912     2

Router-3#sh cdp neighbors
……<resultado omitido>……
Device ID      Local Intrfce    Holdtme   Capability  Platform  Port ID
Sw-1             Fas0        172        T S     2950     1
Router-1         Ser1        176        R       2620     2
Router-4         Ser0        172        R       2620     1

Router-4#sh cdp neighbors
……<resultado omitido>……
Device ID      Local Intrfce    Holdtme   Capability  Platform  Port ID
Router-3         Ser0        166        R       2620     1

 Distance: (default is 110)

ISP#sh cdp neighbors
……<resultado omitido>……
Device ID      Local Intrfce    Holdtme   Capability  Platform  Port ID
Router-1         Ser0        161        R       2620     1
```

2. COMPROBANDO EL PROTOCOLO DE ENRUTAMIENTO HABILITADO

```
Router-1#show ip protocol
Routing Protocol is "ospf 50"
  Sending updates every 90 seconds, next due in 10 seconds
  Invalid after 30 seconds, hold down 0, flushed after 60
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:   ospf 50
  Routing for Networks:
    225.0.0.164 0.0.0.3 area 0
    225.0.0.160 0.0.0.3 area 0
    200.200.100.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    225.0.0.165          110      00:00:00
  Distance: (default is 110)
```

```
Router-2#sh ip protocol
Routing Protocol is "ospf 50"
  Sending updates every 90 seconds, next due in 10 seconds
  Invalid after 30 seconds, hold down 0, flushed after 60
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:   ospf 50
  Routing for Networks:
    225.0.0.160 0.0.0.3 area 0
    225.0.0.128 0.0.0.15 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    225.0.0.161          110      00:00:00
  Distance: (default is 110)

Router-3#sh ip protocol
Routing Protocol is "ospf 50"
  Sending updates every 90 seconds, next due in 10 seconds
  Invalid after 30 seconds, hold down 0, flushed after 60
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:   ospf 50
  Routing for Networks:
    225.0.0.164 0.0.0.3 area 0
    225.0.0.168 0.0.0.3 area 0
    225.0.0.64 0.0.0.63 area 0
    225.0.0.32 0.0.0.31 area 0
    225.0.0.192 0.0.0.31 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    225.0.0.158          110      00:00:00
  Distance: (default is 110)

Router-4#sh ip protocol
Routing Protocol is "ospf 50"
  Sending updates every 90 seconds, next due in 10 seconds
  Invalid after 30 seconds, hold down 0, flushed after 60
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:   ospf 50
  Routing for Networks:
    225.0.0.168 0.0.0.3 area 0
    225.0.0.144 0.0.0.15 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    225.0.0.170          110      00:00:03

DIAGNÓSTICO DE VECINOS OSPF
Router-1#show ip ospf neig
Neighbor ID     Pri   State           Dead Time   Address         Interface
225.0.0.162     0     FULL/           00:00:00    225.0.0.162       FastEthernet0/0

Router-2#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
225.0.0.161     0     FULL/           00:00:00    225.0.0.161       FastEthernet0/0
```

```
Router-3#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
200.200.100.2     0   FULL/           00:00:08    225.0.0.162     Serial0
Router-4#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
225.0.0.169       1   FULL/           00:00:03    225.0.0.169     Serial0
```

4. **TABLA DE ENRUTAMIENTO**:

```
Router-1#show ip route
……<resultado omitido>……
Gateway of last resort is 200.200.100.1 to network 0.0.0.0
C     225.0.0.160/30 is directly connected, FastEthernet0/0
C     225.0.0.164/30 is directly connected, Serial1
C     200.200.100.0/30 is directly connected, Serial0
C     192.168.1.1/0 is directly connected, Loopback0
S*    0.0.0.0/0 [1/0] via 200.200.100.1
O     225.0.0.128/28 [110/11] via 225.0.0.162, 00:00:19, FastEthernet0/0
O     225.0.0.64/26 [110/65] via 225.0.0.166, 00:00:44, Serial1
O     225.0.0.192/27 [110/65] via 225.0.0.166, 00:00:24, Serial1
O     225.0.0.32/27 [110/65] via 225.0.0.166, 00:00:26, Serial1
O     225.0.0.168/30 [110/65] via 225.0.0.166, 00:00:19, Serial1
O     225.0.0.144/28 [110/193] via 225.0.0.166, 00:00:23, Serial1

Router-2#sh ip route
……<resultado omitido>……
Gateway of last resort is not set
C     225.0.0.160/30 is directly connected, FastEthernet0/0
C     192.168.1.22/0 is directly connected, Loopback0
O     225.0.0.164/30 [110/11] via 225.0.0.161, 00:00:50, FastEthernet0/0
O     225.0.0.64/26 [110/85] via 225.0.0.161, 00:00:15, FastEthernet0/0
O     225.0.0.192/27 [110/85] via 225.0.0.161, 00:00:30, FastEthernet0/0
O     225.0.0.32/27 [110/85] via 225.0.0.161, 00:00:40, FastEthernet0/0
O     225.0.0.168/30 [110/85] via 225.0.0.161, 00:00:45, FastEthernet0/0
O     200.200.100.0/30 [110/11] via 225.0.0.161, 00:00:24, FastEthernet0/0
O     225.0.0.144/28 [110/213] via 225.0.0.161, 00:00:27, FastEthernet0/0
C     225.0.0.128/28 is directly connected, FastEthernet0/1

Router-3#sh ip route
……<resultado omitido>……
Gateway of last resort is not set
C     225.0.0.156/30 is directly connected, Serial1
C     225.0.0.64/26 is directly connected, 225.0.0.65
C     225.0.0.192/27 is directly connected, 225.0.0.193
C     225.0.0.32/27 is directly connected, 225.0.0.62
C     225.0.0.160/30 is directly connected, Serial0
O     225.0.0.144/28 [110/65] via 225.0.0.170, 00:00:50, Serial0
C     192.168.1.3/0 is directly connected, Loopback0
O     225.0.0.160/30 [110/65] via 225.0.0.165, 00:00:48, Serial1
O     200.200.100.0/30 [110/65] via 225.0.0.165, 00:00:40, Serial1
O     225.0.0.128/28 [110/139] via 225.0.0.165, 00:00:31, Serial1
```

```
Router-4#sh ip route
……<resultado omitido>……
Gateway of last resort is not set
C    225.0.0.160/30 is directly connected, Serial0
C    225.0.0.144/28 is directly connected, FastEthernet0/0
O    225.0.0.164/30 [110/65] via 225.0.0.169, 00:00:16, Serial0
O    225.0.0.64/26 [110/65] via 225.0.0.169, 00:00:33, Serial0
O    225.0.0.192/27 [110/65] via 225.0.0.169, 00:00:21, Serial0
O    225.0.0.32/27 [110/65] via 225.0.0.169, 00:00:47, Serial0
O    225.0.0.160/30 [110/193] via 225.0.0.169, 00:00:49, Serial0
O    225.0.0.128/28 [110/267] via 225.0.0.169, 00:00:38, Serial0
O    200.200.100.0/30 [110/193] via 225.0.0.169, 00:00:32, Serial0
C    192.168.1.4/0 is directly connected, Loopback0

ISP#sh ip route
……<resultado omitido>……
Gateway of last resort is not set
C    150.13.2.1/0 is directly connected, Loopback0
C    200.200.100.0/30 is directly connected, Serial0
S    225.0.0.0/24 [1/0] via 200.200.100.2
```

5. CONFIGURACIÓN FINAL DE LOS ROUTERS

```
Router-1#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-1
!
ip subnet-zero
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
 no ip directed broadcast
!
interface Serial0
 ip address 200.200.100.2 255.255.255.252
 no ip directed-broadcast
 clock rate 64000
 ip ospf cost 64
!
interface Serial1
 ip address 225.0.0.165 255.255.255.252
 no ip directed-broadcast
 ip ospf cost 64
!
interface FastEthernet0/0
 ip address 225.0.0.161 255.255.255.252
 no ip directed-broadcast
 ip ospf cost 10
```

```
!
router ospf 50
 network 225.0.0.164 0.0.0.3 area 0
 network 225.0.0.160 0.0.0.3 area 0
 network 200.200.100.0 0.0.0.3 area 0
!
ip classless
no ip http server
ip route 0.0.0.0 0.0.0.0 200.200.100.1
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 4
 login
 password ABC
!
no scheduler allocate
end
```

1. CONFIGURACIÓN DEL ROUTER 2

```
Router-2#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
ip subnet-zero
!
interface Loopback0
 ip address 192.168.1.22 255.255.255.255
 no ip directed broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet0/0
 ip address 225.0.0.162 255.255.255.252
 no ip directed-broadcast
 ip ospf cost 10
 ip ospf priority 50
```

```
!
interface FastEthernet0/1
 ip address 225.0.0.129 255.255.255.240
 no ip directed-broadcast
 ip ospf cost 10
!
router ospf 50
 network 225.0.0.160 0.0.0.3 area 0
 network 225.0.0.128 0.0.0.15 area 0
!
ip classless
no ip http server
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 4
 login
 password ABC
!
no scheduler allocate
end
```

2. CONFIGURACIÓN DEL ROUTER 3

```
Router-3#show startup-config
Current configuration : 677 bytes

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-3
!
ip subnet-zero
!
interface Loopback0
 ip address 192.168.1.3 255.255.255.255
 no ip directed broadcast
!
interface Serial0
 ip address 225.0.0.168 255.255.255.252
 no ip directed-broadcast
 ip ospf cost 64
!
interface Serial1
 ip address 225.0.0.166 255.255.255.252
 no ip directed-broadcast
 clock rate 64000
 ip ospf cost 64
!
```

```
interface Serial2
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/0.1 multipoint
 ip address 225.0.0.65 255.255.255.192
!
interface FastEthernet0/0.2 multipoint
 ip address 225.0.0.193 255.255.255.224
!
interface FastEthernet0/0.3 multipoint
 ip address 225.0.0.62 255.255.255.224
!
router ospf 50
 network 225.0.0.156 0.0.0.3 area 0
 network 225.0.0.160 0.0.0.3 area 0
 network 225.0.0.64 0.0.0.63 area 0
 network 225.0.0.32 0.0.0.31 area 0
 network 225.0.0.192 0.0.0.31 area 0
!
ip classless
no ip http server
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 4
 login
 password ABC
!
no scheduler allocate
end
```

3. CONFIGURACIÓN DEL ROUTER 4

```
Router-4#sh startup-config
Current configuration : 677 bytes

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-4
!
ip subnet-zero
!
```

```
interface Loopback0
 ip address 192.168.1.4 255.255.255.255
 no ip directed broadcast
!
interface Serial0
 ip address 225.0.0.170 255.255.255.252
 no ip directed-broadcast
 clock rate 64000
 ip ospf cost 64
!
interface Serial1
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/0
 ip address 225.0.0.145 255.255.255.240
 no ip directed-broadcast
 ip ospf cost 10
!
router ospf 50
 network 225.0.0.168 0.0.0.3 area 0
 network 225.0.0.144 0.0.0.15 area 0
!
ip classless
no ip http server
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 4
 login
 password ABC
!
no scheduler allocate
end
```

```
ISP#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ISP
!
ip subnet-zero
ISP#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname ISP
!
ip subnet-zero
!
interface Loopback0
 ip address 150.13.2.1 255.255.255.255
 no ip directed broadcast
!
interface Serial0
 ip address 200.200.100.1 255.255.255.252
 no ip directed-broadcast
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
no ip http server
ip route 225.0.0.0 255.255.255.0 200.200.100.2
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 4
 login
 password ABC
!
no scheduler allocate
end
```

RESULTADOS DE LA CONFIGURACIÓN EN SWITCH:

1. Diagnóstico inicial

```
Sw-1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S -Switch, H - Host, i - IGMP, r - Repeater
Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
Sw-2           Fas2         167          T S     2950      11
Router-3         Fas1          177          R       2620      4

Sw-2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S -Switch, H - Host, i - IGMP, r - Repeater
Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
Sw-1           Fas1         176          T S     2950      12
Sw-3           Fas2         179          T S     2950      12

Sw-3#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S -Switch, H - Host, i - IGMP, r - Repeater
Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
Sw-2           Fas2         178          T S     2950      12
```

2. Verificación de VLAN

```
Sw-1#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12
30   30                                active    Fa0/2
10   10                                active    Fa0/3
20   20                                active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
……<resultado omitido>……

Sw-2#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12
30   30                                active
10   10                                active    Fa0/3
20   20                                active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
……<resultado omitido>……
```

```
Sw-3#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12
30   30                                active
10   10                                active    Fa0/3
20   20                                active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

.....<resultado omitido>.....
```

3. Características VTP:

```
Sw-1#sh vtp status
VTP Version              : 2
Configuration Revision   : 2
Maximum VLANs supported locally : 64
Number of existing VLANs : 8

VTP Operating Mode       : Server
VTP Domain Name          : ABC
VTP Pruning Mode         : Disabled
VTP V2 Mode              : Disabled
VTP Traps Generation     : Disabled
MD5 digest               : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)

Sw-2#sh vtp status
VTP Version              : 2
Configuration Revision   : 2
Maximum VLANs supported locally : 64
Number of existing VLANs : 8

VTP Operating Mode       : Client
VTP Domain Name          : ABC
VTP Pruning Mode         : Disabled
VTP V2 Mode              : Disabled
VTP Traps Generation     : Disabled
MD5 digest               : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)

Sw-3#sh vtp status
VTP Version              : 2
Configuration Revision   : 2
Maximum VLANs supported locally : 64
Number of existing VLANs : 8
```

```
VTP Operating Mode          : Client
VTP Domain Name             : ABC
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)
```

4. Características STP:

```
Sw-1#show spanning-tree
Vlan 1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000C.1209.1375
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 1)
             Address     000C.2018.9057
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface       Port ID                 Designated              Port ID
Name            Prio.Nbr     Cost Sts     Cost Bridge ID          Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1           100.1        100 FWD       0 32768 000C.2018.9057 100.1
Fa0/12          100.12        20 FWD       0 32768 000C.1209.1375 100.12

Sw-2#sh spanning-tree
Vlan 1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000C.1209.1375
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 1)
             Address     000C.1625.2062
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface       Port ID                 Designated              Port ID
Name            Prio.Nbr     Cost Sts     Cost Bridge ID          Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/11          100.11       100 FWD       0 32768 000C.1625.2062 100.11
Fa0/12          100.12         1 FWD       0 32768 000C.1209.1375 100.12


Sw-3#sh spanning-tree
Vlan 1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000C.1209.1375
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
 Bridge ID  Priority    32768  (priority 32768 sys-id-ext 1)
        Address     000C.1209.1375
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300

Interface       Port ID              Designated            Port ID
Name            Prio.Nbr     Cost Sts     Cost Bridge ID         Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/12          100.12       100 FWD       0 32768 000C.1209.1375 100.12
```

CONFIGURACIÓN FINAL

- **Sw-1 (primer piso)**

```
!
ip subnet-zero
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode trunk
 no ip address
!
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 30
 no ip address
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 10
 no ip address
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 20
 no ip address
!
……<resultado omitido>……
!
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown
!
vlan 30 name 30
vlan 10 name 10
vlan 20 name 20
!
ip classless
no ip http server
!
line con 0
 login
 transport input none
 password class
line aux 0
line vty 0 15
 login
 password ABC
!
no scheduler allocate
end
```

- **Sw-2 (segundo piso)**

```
Sw-2#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sw-2
ip name-server 0.0.0.0
!
ip subnet-zero
spanning-tree extend system-id
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 10
 no ip address
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 20
 no ip address
!
……<resultado omitido>……
!
interface FastEthernet0/11
 switchport mode trunk
 no ip address
!
interface FastEthernet0/12
 switchport mode trunk
 no ip address
!
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown
!
vlan 30 name 30
vlan 10 name 10
vlan 20 name 20
!
ip classless
no ip http server
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```

- **Sw-3**

```
Sw-3#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sw-3
ip name-server 0.0.0.0
!
ip subnet-zero
spanning-tree extend system-id
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 10
 no ip address
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 20
 no ip address
!
.....<resultado omitido>.....
!
interface FastEthernet0/12
 switchport mode trunk
 no ip address
!
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown
!
vlan 30 name 30
vlan 10 name 10
vlan 20 name 20
!
ip classless
no ip http server
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```

CONCLUSIONES

_____

Capítulo

5 Anexos

I. LAS "LÍNEAS" DE LOS ROUTERS CISCO

Al trabajar con routers y switches Cisco nos familiarizamos con las llamadas "líneas" de acceso al dispositivo ("line", en inglés). Su conocimiento y configuración es un aspecto fundamental de la tarea del administrador de dispositivos.

Las líneas del dispositivo son de dos tipos: los puertos seriales y las conexiones de red virtuales. Para verificar cuáles son las líneas de acceso disponibles en su dispositivo puede utilizar el comando show line.

```
Router#show line
.Tty Typ...Tx/Rx .A Modem.Roty AccO AccI Uses Noise Overruns Int
*.0..CTY..... - ..- ... - .. - .. - .. 0 ....0 .. 0/0 .. -
..1..AUX 9600/9600 - ..- ....- ...- .. - .. 0 ....0 .. 0/0 .. -
..2..VTY ..........- ..- ....- .. - .. - .. 0 ....0 .. 0/0 .. -
..3..VTY ..........- ..- ....- .. - .. - .. 0 ....0 .. 0/0 .. -
..4..VTY ..........- ..- ....- .. - .. - .. 0 ....0 .. 0/0 .. -
..5..VTY ..........- ..- ....- .. - .. - .. 0 ....0 .. 0/0 .. -
..6..VTY ..........- ..- ....- .. - .. - .. 0 ....0 .. 0/0 .. -
```

De acuerdo a lo que se muestra en el resultado, el dispositivo cuenta con un puerto consola (CTY) actualmente en uso (lo marca el asterisco), un puerto auxiliar (AUX) y cinco puertos virtuales (VTY).

El puerto CTY

Es el que conocemos habitualmente como puerto consola. Nos permite realizar la configuración del dispositivo aun cuando no exista un archivo de configuración y no haya ninguna información previa. Se trata de un puerto serie que requiere de la utilización de una terminal con puerto serie conectada al puerto consola mediante un cable consola (rollover) con un adaptador DB9 o RJ45. Este acceso debe ser adecuadamente asegurado utilizando una clave, que puede ser clave única o clave de acceso de un usuario local. Recuerde que esta clave se guarda en el archivo de configuración en texto plano, por lo que si se le desea encriptar, debe utilizarse el servicio de encriptación de claves de Cisco IOS.

Un ejemplo de configuración de este puerto:

```
Router(config)#username usuario password clave
Router(config)#line console 0
Router(config-line)#login local
Router(config-line)#loggin synchronous
Router(config-line)#exec-timeout 5 0
Router(config-line)#_
```

El puerto auxiliar

No todos los dispositivos están equipados con un puerto auxiliar, identificado como AUX. Este puerto puede actuar como un puerto de respaldo al puerto consola; en casos de emergencia podría emplearse para configurar el equipo.

Originalmente esta línea ha sido integrada con el objetivo de posibilitar la conexión de un módem telefónico a través del cual sea posible conectarse al dispositivo utilizando una conexión dial-up. Es un puerto serial que debe tener una contraseña como tal:

```
Router(config)#line aux 0
Router(config-line)#password clave
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 5 0
Router(config-line)#_
```

Los puertos VTY

Se trata de un conjunto de puertos virtuales utilizados para la conexión al dispositivo, vía Telnet, SSH, http o https, para realizar administración in band.

La mayoría de los dispositivos tiene al menos cinco puertos virtuales identificados como VTY 0 a 4. Sin embargo, en la medida en que resulte necesario, se pueden generar más puertos virtuales hasta completar un total de 21 líneas VTY. Un ejemplo de configuración:

```
Router(config)#line vty 0 4
Router(config-line)#password clave
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 5 0
Router(config-line)#transport input ssh
Router(config-line)#exit
```

```
Router(config)#line vty 5 20
Router(config-line)#password clave
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 5 0
Router(config-line)#transport input ssh
Router(config-line)#_
```

Una mala configuración de las líneas de acceso es un riesgo de seguridad importante. Estas líneas siempre deben ser configuradas adecuadamente, de acuerdo a las políticas de acceso definidas.

Por otro lado, cuando alguna de estas líneas de acceso es utilizada, es posible simplemente bloquearla habilitando el requerimiento de clave pero negando la clave en esa línea. Un ejemplo de bloqueo del acceso por puerto auxiliar:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#no password
Router(config-line)#^Z
Router#_
```

El acceso a las líneas de terminal virtual puede ser asegurado utilizando listas de acceso estándar, limitando de esta forma las direcciones IP que podrán acceder por Telnet o SSH al dispositivo:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 205.7.5.0 0.0.0.7
Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
Router(config-line)#^Z
Router#_
```

La configuración completa de todas las líneas de acceso puede verificarse al final del archivo de configuración:

```
Router#show running-config
Building configuration...
!
[se omite parcialmente información]
!
line con 0
.exec-timeout 5 0
.logging synchronous
.login local
.stopbits 1
line aux 0
.exec-timeout 5 0
.password clave
.logging synchronous
.login
.stopbits 1
line vty 0 4
.exec-timeout 5 0
.password clave
.logging synchronous
.login
line vty 5 20
.exec-timeout 5 0
.password clave
.logging synchronous
.login
!
end
```

II. CONFIGURACIÓN RECOMENDADA

Los consejos indicados a continuación son básicamente accesos rápidos y necesarios para utilizar el IOS de Cisco que ayuda a un administrador de red a desarrollar una tarea más eficiente.

1. CONFIGURACIÓN RÁPIDA

El intérprete de comandos de la IOS, aunque parezca poco amigable, puede llegar a ser muy rápido y cómodo para configurar el equipo, ya que tiene algunas funciones interesantes:

a. Aplicación de la ayuda

Lo más importante del uso de la ayuda del IOS es verificar el tipo de entrada o parámetro que requiere un comando. Resumiendo, se listan tres aspectos importantes de la ayuda contextual del IOS:

- Conocer qué parámetros y comandos adicionales admite cierto comando.
- Conocer qué comandos se escriben, comenzando por ciertas letras.
- Conocer la medida en que se toman los parámetros/argumentos de los comandos.

Saber qué comandos tengo disponibles en el modo en que esté configurando (interfaz, enrutador, configuración global, etc.) La ayuda nos puede dar muy buenos consejos, tanto así que en los exámenes de certificación se adicionó el uso de la ayuda.

b. Uso del símbolo de interrogación (?)

Al colocar el símbolo "?" y presionar Enter, el intérprete de comandos nos devuelve un listado de posibles comandos y posibles parámetros de comandos:

```
Router# conf t
Router(config)# interface ?
Serial
Ethernet
Tokenring
Router(config)# interface Serial ?
<0-1> Serial interface number
etc....
```

También nos da los posibles comandos que empiezan por los caracteres escritos:

```
Router# debug i?
interface ip
Router# debug ip p?
packet peer pim policy
.....
```

Cisco ejecuta casi todos sus comandos en tiempo real; esto hace efecto instantáneamente, sin tener que reiniciar el equipo. Con la flecha hacia arriba repetimos comandos anteriores y con la flecha hacia abajo avanzamos comandos.

c. Acceder a otra opción dentro de un submodo

Estando dentro de un submodo de configuración se podrá acceder a otro submodo directamente, sin necesidad de salir del anterior.

```
Router(config)#interface s0/0
Router(config-if)#ip add 192.168.3.1 255.255.255.252
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0, changed state to down
Router(config-if)#router rip      ← [ uso del acceso en otro submodo ]
Router(config-router)#
```

d. Comando RANGE

El comando range facilita la selección de varias interfaces para configurarlas en grupo.

```
Switch(config)#interface range FastEthernet 0/1 – 12 ← [ uso de range ]
Switch(config-if-range)#shutdown
Switch(config-if-range)#^Z
```

e. Uso del comando write (wr)

Permite grabar la configuración rápidamente en la NVRAM, en reemplazo del comando **copy running-config startup-config**.

```
Router#wr ← [ uso del write o wr ]
Building configuration...
[OK]
Router#
```

f. Uso del Tab

Es una opción que permite completar un comando incompleto al escribir las primeras letras. Aun así, si no completamos el comando y no es ambiguo, lo coge igualmente.

```
Router(config)#in  <TAB> ← [ uso del tab ]
Router(config)#interface serial 0/0
Router(config-if)#
```

g. Uso del Ctrl-Z

Permite salir desde cualquier submodo de operación y ubicarse en el modo privilegiado, facilitando el trabajo con los routers.

```
Router(config-if)#^Z  ← [ uso del ctrl-Z ]
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

h. Uso del comando "do"

Permite que se ejecuten comandos del modo privilegiado desde el modo configuración global.

```
Router(config-router)#do show ip prot  ← [ uso del comando do ]
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
…….< resultado omitido>……..
```

i. Eliminando la configuración de una interfaz

Cuando se necesita cambiar la configuración de una interfaz, típicamente tienen que removerse las partes existentes de la configuración ingresando a la interfaz y anteponiendo la palabra "**no**" o, en todo caso, se elimina toda la configuración para luego reiniciar el router. Pero existe la posibilidad de eliminar sólo la configuración en la interfaz dejando los valores por defecto. Use el comando **default interface <*interface_number*>**.

```
interface Serial0
no ip address
encapsulation frame-relay
clock rate 800000
frame-relay intf-type dce
frame-relay route 102 interface Serial2 201
frame-relay route 103 interface Serial3 301
Router#configure terminal
Router(config)#default interface s0        ← [ uso del comando do ]
Building configuration...
Interface Serial1 set to default configuration
*Feb 28 19:04:56: %LINK-3-UPDOWN: Interface Serial0, changed state
to down
Router#show run interface s0
interface Serial0
no ip address
end
```

j. Terminal DCE y CLOCK RATE

Si desea averiguar cuál es el terminal DCE en el cable serial para habilitar el clock rate cuando trabaje, emplee el comando **"show controller serial x/x"** (indique el número de interfaz serial) o en su defecto puede colocar el valor del clock rate a ambos extremos del enlace en cada interfaz serial; el sistema sólo lo empleará en el extremo que lo requiera.

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock  ← [ indicación del terminal DCE ]
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
…….< resultado omitido >……..
```

2. CONFIGURACIÓN NECESARIA:

a. Registro sincrónico (interrupción de línea de comandos)

El registro o log del sistema aparece e interrumpe momentáneamente la línea de comandos, aunque el comando se puede terminar de escribir y ejecutar, lo que más se acostumbra hacer es cancelar o, peor aún, oprimir *Enter* y volverlo a escribir. Esta es una muy mala práctica pues, si sumado a ese comando coexisten varios al mismo tiempo, se generan comportamientos incomprensibles a primera vista. La solución a este problema es el registro sincrónico, es decir, que el registro o log del sistema se sincronice con la petición de entrada (prompt), de tal manera que cuando el IOS avise acerca de algún suceso del sistema, el aviso salga en una línea aparte y el comando escrito siga intacto.

```
line con 0
logging synchrounous
```

b. Terminal como consola (visualizar vía Telnet los menajes de error)

Las terminales virtuales no son susceptibles de generar registro de actividad como la consola. Para que una terminal virtual sirva como consola y nos permita monitorear la actividad del enrutador es necesario programarle el uso de ***terminal monitor***, que envía a la terminal virtual el registro de actividad del sistema como si fuera una consola directamente conectada al puerto de consola. Se tendría el mismo problema de interrupción de los comandos pero si el comando ***logg syn*** se aplica en una VTY, funcionaría igual.

c. Búsqueda de DNS (comandos mal escritos)

Un problema altamente irritante ocurre cuando al escribir mal un comando y presionar seguidamente *Enter*, el router muestra unos mensajes indicando que no se encuentra el DNS o la dirección. Lo que sucede es que cualquier cosa que no sea un comando se interpreta como una intención de hacer Telnet, es decir, la palabra mal escrita se intenta traducir a una dirección IP a la cual se va a enviar una petición de abrir Telnet. Para alterar este comportamiento se usa el comando **no ip domain-lookup** en modo de configuración global.

```
configure terminal
no ip domain-lookup
```

También se podría cambiar el método de transporte a "ninguno", tanto en la línea de consola como en el terminal virtual.

```
line con 0
   transport preferred none
 line vty 0 5
   transport preferred none
```

d. Establecer ALIAS

Se pueden crear alias de comandos que se usan repetidamente y son largos de teclear a pesar de las típicas abreviaciones. Para ello podemos usar el comando alias para crear comandos simples e incluso pasar parámetros a estos alias.

Para crear un alias debemos primero ir a la configuración con **configure terminal**. Por ejemplo, si queremos usar ifconfig para tener listas las interfaces, podemos usar este alias:

```
Router(config)#
Router(config)#alias exec s ahow ip int brief
Router(config)#alias exec sir show ip route
Router(config)#alias exec sr show run
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#sir
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 200.1.1.1, 00:00:12, Serial0/0
C    200.1.1.0/24 is directly connected, Serial0/0
Router#
```

e. El comando reload (programar una restauración automática)

Al configurar en el router, por error podríamos bloquear el acceso permanentemente, por ejemplo, una lista que permita el acceso sólo a ciertos protocolos desde ciertas estaciones y lo estemos haciendo a través de Telnet/SSH. En el momento en que aplicamos la ACL se bloquea nuestro terminal y la única solución sería reiniciar el enrutador, ya que probablemente la configuración no haya sido guardada, pero si adicionalmente el enrutador está en otro país y la ACL bloqueó críticamente el tráfico de nuestros clientes... ¿Qué se hace?

El comando reload nos permite configurar el router para que al cabo de X minutos deshaga los últimos cambios realizados, de modo que en caso de error la configuración vuelve a su estado anterior y tenemos acceso de nuevo al router.

Por ejemplo, resetear en tres minutos:

```
Router#reload in 3
   Reload scheduled in 3 minutes
Proceed with reload? [confirm]y
```

Por supuesto, si realizamos los cambios y todo ha funcionado a la perfección, este reseteo puede ser cancelado:

```
Router#reload cancel
```

f. Habilite una contraseña al puerto auxiliar

En algunas ocasiones el puerto consola puede tener serios problemas que deben ser prevenidos, ya que sin él no podremos acceder a la configuración del equipo. Una recomendación es mantener siempre una contraseña en el puerto auxiliar, ya que puede reemplazar al puerto consola o, en la medida de lo posible, dejar configurado el acceso al terminal virtual.

g. El bloc de notas

Se recomienda tenerlo presente como una herramienta, ya que podemos realizar plantillas de las distintas configuraciones que se hacen (NAT, PAT, Access list, DHCP, etc.), lo cual acelera el trabajo y facilita el diagnóstico de posibles errores.

3. FACILITANDO EL TRABAJO

a. Recuperación de passwords

Sería absurdo tener que llevar el router al fabricante para que limpie la NVRAM o algo así, si no se conoce la contraseña. Existe un procedimiento de "password recovery" en Cisco. Este es el ejemplo del uso del modo rommon:

Paso 1: Encendemos el router y pulsamos Ctrl + Break durante el arranque (primeros 60 segundos). Así entramos en modo rommon:

```
rommon 1>
```

Paso 2: Cambiamos el valor del registro de configuración para que no lea la NVRAM al arrancar:

```
rommon 1> o/r 0x2141 (o confreg 0x2142)
rommon 2>
```

Paso 3: initialize (= i) (rearrancamos).

Paso 4: Al arrancar nos pedirá entrar en modo setup, contestamos que no.

Paso 5: Como no ha leído la NVRAM, la running-config del router está vacía, así que nos ponemos en modo enable sin que nos pida el password.

Paso 6: Vemos o cambiamos el password. Es recomendable cargar startup sobre running y modificar, si hace falta (copy startup run).

Paso 7: Restauramos el valor del registro de configuración con "config-register 0x2102".

Paso 8: Guardamos la configuración, si se ha cambiado, y hacemos un reload.

b. Registro del trabajo por marcas de tiempo

Muchas veces, los acontecimientos router pueden pasar tan rápido que varios eventos suceden en el mismo segundo (especialmente en los routers grandes que tienen una gran cantidad de rutas). Para asegurarse de que su registro pueda decir exactamente lo que sucedió y en qué momento, utilice este comando: *servicio de registro de marcas de tiempo muestran fecha y hora localtime años ms zona horaria.*

Al usar este comando asegúrese de que el router emita todas las marcas de tiempo de los mensajes de registro con la hora actual, la zona horaria (para los que tengan routers remotos en diferentes zonas horarias), la milésima de segundo en que se produjo el suceso y el año. Para aquellos cuyos routers no suelen tener muchos eventos, puede ser agradable saber el año. Esto es lo que aparece como marca de tiempo (sin año):

```
* Oct 21 15:31:54.955 CDT:% LINEPROTO-5-UpDown: protocolo de interfaz de línea de GigabitEthernet0
/ 0, cambiado de estado para derribar
```

Además, puede utilizar la *secuencia* de *números de* orden *de servicio* para incluir un número absoluto que identifique a cada evento y muestre la secuencia en que ocurrieron los hechos. Al introducir este comando se le dice al router que agregue un número junto a cada mensaje de registro, lo que señala también el evento y las órdenes de los eventos por número de secuencia.

c. Comienza con una pizarra limpia

Digamos que ha configurado una interfaz en el router, pero más tarde decide que desea volver a configurarla. Sin tener que quitar lo que se propuso, comando por comando, o sin tener que preguntarse qué comandos ha añadido y fueron predeterminados, usted puede rápidamente hacer una única interfaz de nuevo a su configuración, en un comando. Sólo tiene que utilizar el comando *la interfaz por defecto,* como en *Fa0 interfaz por defecto / 0.*

III. EL REGISTRO DE CONFIGURACIÓN

Es un número de dos bytes que se almacena en la NVRAM y define el modo en el que arranca el router. Normalmente, el router intenta arrancar una imagen de IOS de la memoria Flash, pero podemos cambiar esto y también podemos arrancar el router sin que lea la NVRAM.

Los valores que nos interesan del registro de configuración son los que pueden tomar los cuatro bits menos significativos (bits 0, 1, 2 y 3), y el valor del bit 6:

Valor de los 4 BMS. Significado

0x0 Arranca en modo rommon

0x1 Arranca en modo boot

0x2 a 0xF Examina la NVRAM en busca de algún comando "boot system" y si no lo halla, arranca la primera imagen de la Flash.

Valor del bit 6. Significado

0 (0x00) Arranca leyendo la NVRAM

1 (0x40) Arranca sin leer la NVRAM

De este modo podemos hacer combinaciones (el valor 21h en el primer byte viene por defecto en Cisco, no influye):

Valor del registro. Significado

0x2102 Se carga la IOS de la Flash y se lee NVRAM (por defecto)

0x2142 Se carga IOS de Flash y no se lee NVRAM

0x2101 Modo boot leyendo la NVRAM

0x2141 Modo boot sin leer la NVRAM

> ***Nota**: No se incluyen las combinaciones en modo rommon porque a ese modo se accede más fácilmente interrumpiendo la secuencia de inicio con Ctrl + Break, y además no tiene sentido lo de leer o no la NVRAM ya que en modo rommon nunca se lee.*

Para cambiar el valor del registro de configuración podemos usar el comando (en modo configuración global):

```
Router(config)# config register 0x21XX
```

Luego hacemos un "reload", y si se nos pregunta si queremos guardar la configuración, debemos responder que no.

Hay otro modo de cambiar el valor del registro, lo veremos más adelante (en el ejemplo del modo rommon). Para ver el valor actual del registro, usamos el comando "show version", que nos muestra también datos sobre el hardware y el software del router.

IV. SOLUCIÓN DE PROBLEMAS BÁSICOS

Dentro de las alternativas de diagnóstico para facilitar el trabajo del administrador de red se presentan aspectos básicos para la solución de posibles problemas que pueden ocurrir en un router Cisco. Se clasifican y resuelven problemas.

Es una introducción para realizar la configuración básica de un router Cisco y el IOS. Se divide en tres secciones:

1. **Problemas de hardware**

   Los problemas de hardware suelen referirse a los controladores de interfaces, módulos de la RAM, procesador del router, un cable de interfaz mal conectado e incluso el ventilador.

   - Si el ventilador no funciona, el router se calentará y se reiniciará (no exponga el router a temperaturas superiores a 37 °C).
   - Si el router se detiene de forma anormal, puede utilizarse el comando **show stacks** para recuperar los mensajes de error que se hayan guardado en el monitor de la ROM en el momento de la detención. El help desk de Cisco puede ayudarle a determinar la causa del error con esta información. Así mismo, es buena costumbre proteger el router contra las caídas y picos de suministro eléctrico, mediante un SAI.
   - Puede que el router no disponga de memoria RAM o procesador suficiente para gestionar el tráfico de los paquetes. Uno de los métodos que utilizan los administradores para identificar cuellos de botella es utilizar algún tipo de paquete de software de gestión de red. CiscoWorks es un ejemplo de paquete de software de gestión de red que proporciona varias herramientas para controlar interconexiones de redes y resolver los posibles problemas que puedan surgir.

2. **Problemas de interfaz**

   - Los problemas de conectividad en una red Lan pueden estar relacionados con la longitud del cable físico de la red, el cable roto, etc. Si la luz no se enciende significará que el cable está mal, el puerto del hub está estropeado, o la interfaz del router o de la tarjeta de red conectada a dicho puerto no funciona.
   - Los dispositivos de conexión WAN también pueden presentar problemas, como el equipo de conmutación proporcionado por el proveedor de servicios, donde poco se podrá hacer. Lo más recomendable es que los administradores de redes construyan sistemas de tolerancia a las fallas mediante la configuración de conexiones redundantes.
   - Los problemas relacionados con Ethernet pueden derivarse de un exceso de colisiones en red, debidas habitualmente a roturas en el cable, cables que superan la longitud máxima permitida, a un excesivo tráfico de difusión o al funcionamiento defectuoso de alguna tarjeta de red. El comando **show interfaces** [interfaz] permite consultar las estadísticas referidas a una interfaz.
   - **Ethernet 0 is up, Line Protocol is Up**. Esto indica que la interfaz está activada y que los protocolos Ethernet creen que se puede utilizar la línea. Si la interfaz está desactivada, compruebe la conexión Lan con la interfaz. Puede utilizar el comando shut (para desactivar la interfaz) y después, el comando no shut para volver a activarla.
   - **Serial 0 is Up, Line Protocol is Up**. El parámetro **Serial 0 is Up** indica que la interfaz está activa. Si la interfaz está desactivada, puede deberse a un problema con la conexión entre el router y el CSU/DSU, como la conexión del cable o la línea telefónica. El parámetro **Line Protocol is Up** indica que los protocolos WAN en uso creen que la línea puede utilizarse. Si el protocolo de línea está desactivado, puede deberse a que el router está mal configurado (utilice el comando show running-config), aunque podría tratarse también de un problema de la línea o del equipo de conmutación del proveedor.
   - **Hardware Address**. Muestra la dirección MAC.

- **Internet Address**. Muestra la dirección IP y la máscara de subred.
- **MTU**. Es la unidad máxima de transmisión para la interfaz, expresada en bytes.
- **BW**. Corresponde al ancho de banda para la interfaz, expresado en kilobits por segundo.
- **Rely**. Se trata de un parámetro para evaluar la fiabilidad de la línea, siendo 255/255 el máximo de fiabilidad. La fiabilidad suele estar afectada debido a cortes en la línea y otros problemas.
- **Load**. Este parámetro mide la carga actual que soporta la interfaz. Un valor de 255/255 representa una interfaz totalmente saturada.
- **Encapsulation**. Indica el tipo de trama asignado a la interfaz. ARPA es la opción predeterminada para Ethernet y corresponde al tipo de trama 802.2.
- **Collisions**. Muestra el número de colisiones controladas por la interfaz. Un número grande de colisiones indica que puede existir algún tipo de problema físico en la red, como un corte en un cable o un funcionamiento defectuoso de la tarjeta de interfaz.
- **CRC**. Para interfaces Lan. Este parámetro muestra el número de pruebas de redundancia cíclica que han fallado en los paquetes entrantes. Normalmente indica si la línea está soportando muchas interferencias o si el cable serie conectado del router al CSU/DSU es demasiado largo.
- **Last input**. Número de horas, minutos y segundos desde que fue recibido con éxito el último paquete por una interfaz. Es útil para saber cuándo ha fallado una interfaz.
- **Output**. Número de horas, minutos y segundos desde que fue transmitido con éxito el último paquete por una interfaz. Es útil para conocer cuándo ha fallado una interfaz.
- **5 minute input rate, 5 minute output rate**. Velocidades de entrada y salida de los últimos cinco minutos. Permiten obtener una media aproximada del tráfico por segundo en un momento concreto.
- **Packets input**. Número total de paquetes recibidos sin error por el sistema.
- **Bytes input**. Número total de bytes, incluido el encapsulado MAC y datos, en paquetes recibidos sin errores.
- **No buffer**. Número de paquetes recibidos que han sido descartados por no haber espacio suficiente en el búfer para la interfaz.
- **Received... broadcasts**. Número total de difusiones recibidas por la interfaz. Un umbral aproximado podría ser menor del 20% del número de paquetes recibidos.
- **Runts**. Número de paquetes que han sido descartados debido a que su tamaño es menor al tamaño mínimo de paquete permitido, por ejemplo, cualquier paquete Ethernet menor de 64 bytes. Suelen estar causados por colisiones.
- **Giants**. Número de paquetes que han sido descartados por sobrepasar el tamaño máximo de paquete, por ejemplo, cualquier paquete Ethernet mayor de 1518 bytes.

- Puede utilizar un dispositivo de control denominado **caja de escape** para determinar si está recibiendo una señal desde el CSU/DSU. Desconecte el CSU/DSU del router y conéctelo a la caja de escape. Si no obtiene una señal, es posible que la línea contratada no esté bien conectada al CSU/DSU o que no funcione.

3. Problemas de protocolo

- Si una estación de trabajo puede comunicarse con las máquinas de su subred, pero no con el resto de máquinas de otras subredes, compruebe la puerta de enlace configurada en dicha estación de trabajo.
- Utilice el comando **show ip interfaces** para asegurarse de que todas las interfaces del router se han configurado con una dirección IP. Diagnostique con precaución respecto al uso de las listas de control de acceso.

- Utilice el comando **show ip route** para determinar si el router está activo para enrutamiento. Puede utilizar el comando **show running-config** para comprobar si está activo algún protocolo de enrutamiento.
- Dos herramientas muy útiles para comprobar las conexiones son ping y trace. **Ping** envía un paquete ICMP con petición de eco a la dirección IP indicada, y si dicha dirección recibe el paquete, pasa a responder devolviendo el paquete a su origen. Existe una versión ampliada del comando ping que permite establecer el tamaño del paquete y otros parámetros. Los tiempos mostrados por ping están medidos en milisegundos. **Trace** permite consultar la ruta que seguirán los paquetes desde el origen hasta el destino. Con ello se puede determinar si los routers que normalmente participarán en la ruta está activados o no.
- El comando debug es muy sencillo pero consume muchos recursos del router, como la memoria, por lo que conviene desactivarlo. Para activar la depuración ejecutaremos el comando **debug…**, mientras que para detenerla ejecutaremos **no debug all**.
- Cualquier administrador de red debe contar con un mapa de red actualizado que abarque a ésta por completo y que incluya el esquema de direccionamiento y la ubicación de los dispositivos como routers, puentes y servidores. Crear un mapa es muy sencillo. Las herramientas de creación de diagramas de red, como Visio Standard, facilitan la construcción de dichos diagramas. Otras versiones de Visio, como Visio Enterprise, proporcionan todos los iconos que se requieren para representar todos y cada uno de los dispositivos de red que se comercializan actualmente, permitiendo así crear diagramas comprensibles para cualquier administrador de red.

V. COMANDOS DE VERIFICACIÓN

1. Atajos útiles "sh" del IOS de Cisco

Muchas veces, cuando hacemos un "show running-config" o lo que es más común "sh run", no queremos ver todo sino un parte de la configuración; para ello hay algunos atajos muy útiles que no siempre se recuerdan:

- **show run interface:**

```
router# sh run int fa0/0
Building configuration...
Current configuration : 93 bytes
!
interface FastEthernet0/0
ip address 10.1.2.1 255.255.255.0
duplex auto
speed auto
end
```

- **show run | section:**

```
router#sh run | section interface
interface FastEthernet0/0
ip address 10.1.2.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
ip address 192.168.4.1 255.255.255.0
duplex auto
speed auto
```

- **show run | begin:**

```
router#sh run | begin interface
interface FastEthernet0/0
ip address 10.1.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.4.1 255.255.255.0
duplex auto
speed auto
!
ip http server
no ip http secure-server
ip classless
!
control-plane
!
!
–More–
```

- **show run | include:**

```
router# sh run interface f0/0 | include ip
ip address 10.1.1.1 255.255.255.0
```

- **show ip interface brief:**

```
router#sh ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.1.1.1 YES manual up up
FastEthernet1/0 192.168.1.1 YES manual up up
```

- **Mientras se está haciendo un "sh run" se puede usar el carácter "/" para hacer una búsqueda específica:**

```
router#sh run
Building configuration...
Current configuration : 663 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname blog_demo
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
!
!
!
ip cef
ip ips po max-events 100
/192.168
filtering...
ip address 192.168.4.1 255.255.255.0
duplex auto
speed auto
!
ip http server
```

2. Mostrar el ancho de banda de interfaces Cisco

Una forma simple y sencilla de mostrar el ancho de banda de las interfaces configuradas en un router es la siguiente:

```
show interface | include protocol|BW
```

Si la usamos muy a menudo podemos crear un alias:

```
alias exec bw show interface | include protocol|BW
```

Entonces, con **bw** tendremos el mismo resultado.

Un ejemplo del resultado:

```
router#show interface | include protocol|BW
FastEthernet0/0 is administratively down, line protocol is down
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
Serial1/0 is up, line protocol is up
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
Serial1/1 is up, line protocol is up
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
Serial1/2 is up, line protocol is up
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
Serial1/3 is administratively down, line protocol is down
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
Loopback0 is up, line protocol is up
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
```

VI. SEGURIDAD BÁSICA

Cisco IOS brinda múltiples formas de asegurar el acceso a las posibilidades de administración de los dispositivos (básicamente, router, switches y AP). Se resumen las principales formas de aplicar seguridad básica a los equipos. Todas las opciones presentadas a continuación se muestran aplicadas de una u otra manera en los diferentes laboratorios de este libro.

1. Niveles de acceso

La interfaz de línea de comando de Cisco IOS utiliza un acceso de niveles jerárquicos: modo EXEC usuario y modo EXEC privilegiado. Se establecen dos niveles básicos de permisos de acceso: acceso de nivel usuario y acceso de nivel privilegiado.

El acceso a modo privilegiado puede ser bloqueado utilizando una clave denominada "clave de modo enable" que puede ser encriptada o no:

```
Router(config)#enable password [clave]
Router(config)#enable secret [clave]
```

Ambas claves son requeridas para acceder al modo privilegiado. Sin embargo, la enable password se guarda en formato de texto plano en el archivo de configuración, mientras que la enable secret se guarda encriptada utilizando MD5.

Por su parte, el acceso a modo usuario se asegura utilizando claves de acceso en las diferentes "líneas": consola, auxiliar o terminal virtual.

En estas líneas de acceso hay diferentes formas de configurar claves de acceso.

2. Clave simple de acceso al modo usuario

En cada una de las líneas de acceso (consola, auxiliar, terminal virtual) se puede asegurar el acceso utilizando una clave simple.

```
Router(config)#line vty 0 4
Router(config-line)#password [clave]
Router(config-line)#login
```

El primer comando define una clave y el comando login indica al dispositivo que debe mostrar el prompt requiriendo el ingreso de la clave cuando se intenta el acceso por terminal virtual (Telnet).

La clave se guarda en el archivo de configuración, en formato de texto plano.

3. Acceso utilizando usuario y clave

El acceso puede asegurarse también utilizando usuario y clave:

```
Router(config)#username [user] secret 0 [clave]
Router(config)#line vty 0 4
Router(config-line)#login local
```

Genera un usuario y una clave que se guarda encriptada utilizando MD5 en el archivo de configuración. Ese usuario y esa clave se aplican a la línea de acceso utilizando el comando login local.

4. Asignación de niveles de privilegio por usuario

Cisco IOS permite configurar 16 niveles de usuario diferente (0 a 15).

- Usuario nivel 0 - Sólo accede a modo usuario.
- Usuario nivel 1 al 14 - Se pueden asignar diferentes comandos para cada nivel.

- Usuario nivel 15 - Acceso a modo privilegiado completo.

La configuración de diferentes niveles de acceso es particularmente útil en entornos en los que diferentes técnicos tienen asignadas diferentes tareas.

Para configurar un usuario con permiso de utilización de un conjunto limitado de comandos de nivel privilegiado, siga este procedimiento:

```
Router(config)#privilege exec level [nivel] [comando]
Router(config)#username [user] privilege [nivel] secret 0 [clave]
Router(config)#line vty 0 4
Router(config-line)#login local
```

También es posible generar niveles de privilegios diferentes y asociarlos directamente a una clave de acceso simple a modo privilegiado:

```
Router(config)#privilege exec level [nivel] [comando]
Router(config)#enable secret level [nivel] [clave]
```

5. Asignación de accesos basados en roles

Cisco IOS también permite definir plantillas o roles con conjuntos de comandos, cada uno asegurado con su clave de acceso.

Esta característica de configuración requiere de la habilitación previa de AAA (Authentication, Authorization, Accounting).

```
Router#enable view
Router#configure terminal
Router(config)#aaa new-model
Router(config)#parser view [nombre]
Router(config-view)#secret 0 [clave]
Router(config-view)#command exec include [comando]
Router(config-view)#command configure include [comando]
```

Una vez configurado el perfil deseado, el acceso a modo privilegiado se logra utilizando el siguiente procedimiento:

```
Router#enable view [nombre]
Password: [clave]
Router(config)#_
```

Al solicitar la ayuda contextual de IOS (?), el usuario sólo visualizará los comandos habilitados para el perfil que utilizó para el login.

6. Use claves complejas (robustas) y encripte las claves en texto plano

Asegúrese de utilizar claves largas y con caracteres alfanuméricos, lo que reduce la posibilidad de que sean violadas por un ataque de fuerza bruta. Este comando Cisco IOS le permite asegurar una longitud de caracteres mínima para cada clave:

```
Router(config)#security password min length 6
```

Una vez configurada esta opción, cuando intentemos introducir una contraseña que sea inferior a lo configurado nos saldrá un aviso:

```
Router(config)#security passwords min-length 10
Router(config)#enable password cisco
% Password too short - must be at least 10 characters. Password configuration failed
```

Asegúrese de que todas las claves estén encriptadas, al menos con un algoritmo de encriptación básico:

```
Router(config)#service password encryption
```

Se pueden prevenir intentos de acceso por fuerza bruta estableciendo parámetros de tiempo para el ingreso de claves en el dispositivo. En este ejemplo se define que el acceso se bloquee por 180 segundos cuando se realicen tres intentos fallidos en un intervalo de 30 segundos.

```
Router(config)#login block for 180 attempts 3 within 30
```

- Para establecer un límite de tiempo de inactividad al final de la cual se cerrará la sesión:

```
Router(config line)#exec timeout [min] [seg]
```

Políticas recomendadas:

- Aunque lo recomendable es usar un sistema de autenticación remoto, como puede ser Radius o Tacacs, siempre debemos tener al menos un usuario local.
- Utilice claves robustas de al menos 10 caracteres alfanuméricos.
- Es aconsejable incluir mayúsculas/minúsculas y símbolos.
- Las claves no deben ser palabras del diccionario.
- Para asegurar el acceso a modo privilegiado utilice siempre la enable secret.
- Active el servicio de encriptación de claves para asegurarse de que no queden claves en texto plano visibles en el archivo de configuración.
- Cambie las claves periódicamente.
- Incluya un mensaje de acceso (banner) advirtiendo que se monitoreará y perseguirá el acceso no autorizado.

7. Desactive aquellos servicios o protocolos que sean innecesarios

Por defecto, los dispositivos Cisco activan diversos servicios que son opcionales. Estos servicios son potenciales puntos de ataques de seguridad, ya que permiten acceder a información del dispositivo. Si no son utilizados, estos servicios pueden ser fácilmente desactivados:

```
Protocolo CDP:
Router(config)#no cdp run

Configuración remota:
Router(config)#no service config

Servicio finger:
Router(config)#no service finger

Servicio web:
Router(config)#no ip http server
```

```
Protocolo SNMP:
Router(config)#no snmp-server

Protocolo BOOTP:
Router(config)#no ip bootp server

Servicios TCP:
Router(config)#no service tcp-small-servers

Servicios UDP:
Router(config)#no service udp-small-servers
```

8. Deshabilite las interfaces que no estén en uso

Las interfaces que no se utilizan deben estar administrativamente deshabilitadas utilizando el comando shutdown. En los routers Cisco, éste es el estado por defecto; por el contrario, en los switches Catalyst, todos los puertos están habilitados por defecto. En las interfaces en uso, si no son necesarios, conviene desactivar los siguientes servicios:

```
Router(config-if)#no ip proxy arp
Router(config-if)#no ip directed broadcast
Router(config-if)#no ip maskreply
```

9. Mantenga control del tráfico que atraviesa el router

Básicamente, se debiera bloquear todo tráfico innecesario. Sin embargo, muchas veces es difícil determinar el tráfico necesario.

Pero hay tráfico que ciertamente no debiera ingresar o circular. Por ejemplo, cuando la red tiene un router a través del cual se conecta a Internet; este dispositivo no debiera recibir desde Internet tráfico que se origine en una dirección IP privada. Para esto, se puede implementar la siguiente lista de acceso, suponiendo que la interfaz a través de la cual el router se conecta a Internet es la interfaz serial 0/0:

```
Router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
Router(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
Router(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
Router(config)#interface serial 0/0
Router(config-if)#description acceso a Internet
Router(config-if)#ip access-group 101 in
```

10. Mantenga los archivos log

Para mantener un control del tráfico que es bloqueado por las listas de acceso, es conveniente utilizar los archivos log. Estos archivos también pueden mantener un registro de los cambios de configuración y errores.

Para mantener estos archivos almacenados en el dispositivo, el procedimiento es el siguiente:

```
Router(config)#logging on
Router(config)#logging buffered 16384
```

De este modo se reserva un espacio de 16 MB en la memoria RAM del dispositivo.

El problema de guardar estos archivos en el router es que en caso de un reinicio del dispositivo se pierden estos archivos. Por eso conviene almacenarlos en un servidor que puede incluso ser un servidor común a todos los dispositivos de la red.

El comando para identificar este servidor es:

```
Router(config)#logging [ip]
```

11. Marca horaria

Un elemento muy importante de información en los archivos log es la marca horaria de los sucesos. Esta marca horaria puede tomarse a partir del reloj interno del dispositivo. Sin embargo, si hay varios dispositivos, es muy importante que todos tomen su marca horaria de un único servidor para poder hacer las comparaciones que puedan ser necesarias. Para activar este servicio utilice el siguiente comando:

```
Router(config)#service timestamps log datetime msec
Router(config)#ntp server server.ntp.address
```

12. Control del acceso remoto

Es conveniente limitar las posibilidades de acceso remoto a la administración de los dispositivos.

Una posibilidad es limitar las direcciones IP y protocolos que se utilizan para acceder a las terminales virtuales. Por ejemplo, para permitir el acceso exclusivamente desde la red local:

```
Router(config)#access-list 10 permit 192.168.2.0 0.0.0.255
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
```

13. Utilice SSH para el acceso remoto

No es recomendable el uso de Telnet o http para la administración de los dispositivos, dados los riesgos de seguridad que esto entraña.

Es altamente recomendable utilizar SSH (Secure Shell) para la administración remota de los dispositivos, ya que SSH viaja encriptado. Para habilitar SSH en un dispositivo siga los siguientes pasos:

```
Router(config)#hostname [nombre]
Router(config)#ip domain-name [nombre]
Router(config)#crypto key generate rsa
Router(config)#ip ssh timeout 60
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
```

***Nota**: Antes de intentar esta implementación, verifique que su versión y el paquete de Cisco IOS soporten SSH.*

14. Establecer seguridad de los protocolos de enrutamiento y otros servicios opcionales

A fin de evitar ataques que signifiquen modificaciones no autorizadas de las tablas de enrutamiento es recomendable utilizar protocolos que soporten una autenticación con claves encriptadas.

Por ejemplo, se puede configurar OSPF para que utilice claves encriptadas:

```
Router(config-if)#ip ospf message-digest key [1-255] md5 [1-7] [clave]
Router(config)#router ospf 1
Router(config-router)#area 0 authentication message-digest
```

15. Prevenga los ataques de denegación de servicio

Un modo simple de prevenir ataques DoS comunes es limitar el ancho de banda utilizado por los paquetes ICMP. El protocolo ICMP suele ser utilizado para inundar la red causando una denegación de servicio. Para prevenir este tipo de ataque se pueden utilizar los comandos que se indican a continuación en cada interfaz, con el fin de de limitar el ancho de banda que será ocupado por el protocolo.

En este caso, limitaré a 20 Kbps la disponibilidad para tráfico de ping en la interfaz serial 0/0 que tiene un ancho de banda total de 64 Kbps. Esto en la realidad depende en cada caso del ancho de banda de cada enlace y la proporción de ese ancho de banda que se desea asignar como máximo a estos protocolos.

```
Router(config)#access-list 101 permit icmp any any echo-reply
Router(config)#access-list 101 permit icmp any any echo
Router(config)#interface serial 0/0
Router(config-if)#rate-limit input access-group 101 20000 8000 8000 conform-action transmit exceed-
action drop
```

Tenga en cuenta que la prevención de ataques de DoS es una tarea más compleja que debe enmarcarse en el contexto de políticas e implementaciones de seguridad. Este es solamente un consejo para lograr una prevención básica.

VII. LISTA DE COMANDOS

MODO EXEC USUARIO

Comando	Descripción
connect {*dirección_ip*|nombre}	Permite conectarse remotamente a un host.
disconnect *conexión*	Desconecta una sesión Telnet establecida desde el router.
enable	Ingresa al modo EXEC Privilegiado.
logout	Sale del modo EXEC.
ping {*dirección_ip*|*nombre*}	Envía una petición de eco para diagnosticar la conectividad básica de red.
resume conexión	Resume una sesión Telnet interrumpida con la secuencia Ctrl+Shift+6 y X.
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación.
show cdp entry [*|*nombre_dispositivo*] [protocol|version]}	Muestra información acerca de un dispositivo vecino registrado en una tabla CDP.
show cdp interfaces [*tipo número*]	Muestra información acerca de las interfaces en las que CDP está habilitado.
show cdp neighbors [*tipo número*] [detail]	Muestra los resultados del proceso de descubrimiento de CDP.
show clock	Muestra la hora y fecha del router.
show history	Muestra el historial de comandos ingresados.
show hosts	Muestra una lista en caché de los nombres de host y direcciones.
show ip interface brief	Muestra un breve resumen de la información y del estado de una dirección IP.
show ip rip database	Muestra el contenido de la base de datos privada de RIP.
show ip route [*dirección |protocolo*]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro dirección permite acotar, exclusivamente a la dirección ingresada, la información que se desea visualizar. El parámetro protocolo permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo: *rip*, *igrp*, *static* y *connected*.
show sessions	Muestra las conexiones Telnet establecidas en el router.
show version	Muestra información sobre el Cisco IOS y la plataforma.
telnet {*dirección_ip*|*nombre*}	Permite conectarse remotamente a un host.
terminal editing	Reactiva las funciones de edición avanzada.
terminal history size *numero_líneas*	Establece el tamaño del buffer del historial de comandos.
terminal no editing	Deshabilita las funciones de edición avanzada.
traceroute *dirección_ip*	Muestra la ruta tomada por los paquetes hacia un destino.

MODO EXEC PRIVILEGIADO

Comando	Descripción
clear cdp counters	Restaura los contadores de tráfico CDP a cero.
clear cdp table	Elimina la tabla CDP de información de los vecinos.
clear counters	Despeja los contadores de las interfaces.
configure memory	Carga información de configuración de la NVRAM.
configure terminal	Configura la terminal manualmente desde la terminal de consola.
copy flash tftp	Copia la imagen del sistema desde la memoria Flash a un servidor TFTP.
copy running-config startup-config	Guarda la configuración activa en la NVRAM.
copy running-config tftp	Almacena la configuración activa en un servidor TFTP.
copy tftp flash	Descarga una nueva imagen desde un servidor TFTP en la memoria Flash.
copy tftp runnig-config	Carga la información de configuración desde un servidor TFTP.
debug cdp adjacency	Muestra información recibida de vecinos CDP.
debug cdp events	Muestra información sobre eventos CDP.
debug cdp ip	Muestra información CDP específica de IP.
debug cdp packets	Muestra información relacionada a los paquetes CDP.
debug ip igrp events	Muestra todos los eventos IGRP que se están enviando y recibiendo en el router.
debug ip igrp transactions	Muestra las actualizaciones IGRP que se están enviando y recibiendo en el router.
debug ip rip	Muestra información sobre las actualizaciones de enrutamiento RIP mientras el router las envía y recibe.
debug ip rip [events]	Muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe.
disable	Sale del modo EXEC Privilegiado hacia el modo EXEC Usuario.
erase flash	Borra el contenido de la memoria Flash.
erase startup-config	Borra el contenido de la NVRAM.
no debug all	Desactiva todas las depuraciones activadas en el dispositivo.
reload	Reinicia el router.
setup	Entra a la facilidad de diálogo de configuración inicial.
show access-lists [*Nro_ACL*|*Nombre_ACL*]	Muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número de ACL como opción a este comando.
show arp	Muestra la asignación de direcciones IP a MAC a la interfaz del router.
show cdp traffic	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos, y los errores de checksum.

show controllers serial [*número*]	Muestra información importante como el tipo de cable que se encuentra conectado.
show debugging	Muestra información acerca de los tipos de depuración que están habilitados.
show flash	Muestra la disposición y el contenido de la memoria Flash.
show interfaces [*tipo número*]	Muestra estadísticas para la/las interfaces indicadas.
show ip interface [*tipo número*]	Muestra los parámetros de estado y globales asociados a una interfaz.
show ip protocols [summary]	Muestra los parámetros y estado actual del proceso de protocolo de enrutamiento activo.
show memory	Muestra estadísticas acerca de la memoria del router, incluyendo estadísticas de memoria disponible.
show processes	Muestra información acerca de los procesos activos.
show protocols	Muestra los protocolos de capa 3 configurados.
show running-config	Muestra la configuración actual en la RAM.
show sessions	Muestra las conexiones Telnet establecidas en el router.
show stacks	Controla el uso de la pila de procesos y rutinas de interrupción, y muestra la causa del último rearranque del sistema.
show startup-config	Muestra la configuración que se ha guardado, que es el contenido de la NVRAM.
terminal monitor	Si se utiliza una sesión por Telnet para examinar el router, entonces permite redirigir el resultado y los mensajes del sistema hacia la terminal remota.
undebug all	Desactiva todas las depuraciones activadas en el dispositivo.

MODO DE CONFIGURACIÓN GLOBAL

Comando	Descripción
access-list *Nro_ACL* {permit|deny} *Origen*	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que lleguen desde un *Origen*. Este último parámetro puede ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP, o el wildcard any.
access-list *Nro_ACL* {permit|deny} *Proto Origen Destino* [*Operador Nro_puerto*] [established][echo |echo-reply]	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que lleguen desde un *Origen* y vayan hacia un *Destino*. *Proto* identifica el protocolo a verificar. *Origen y Destino* pueden ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP, o el wildcard any. *Operador* puede ser lt (menor que), gt (mayor que), eq (igual a) o neq (distinto de). *Nro_puerto* indica el puerto TCP o UDP. El parámetro established permite el paso de tráfico cuando hay una sesión establecida. En el caso del protocolo ICMP se puede utilizar echo o echo-reply.
Banner motd #*mensaje del día*#	Configura un cartel con un mensaje del día. Ejemplo: banner motd #Bienvenido#

boot system flash [*nombre_imagen_IOS*]	Especifica que el router cargue el IOS desde la Flash. Ejemplo: boot system flash c2500-IOS.
boot system rom	Especifica que el router cargue el IOS desde la ROM.
boot system tftp *nombre_imagen_IOS dir_IP_server_tftp*	Especifica que el router cargue el IOS desde un servidor TFTP. Ejemplo: boot system tftp c2500-IOS 24.232.150.1
cdp run	Habilita CDP globalmente en el router.
clock set *hh:mm:ss mes día año*	Modificar la fecha y hora del router. Ej: clock set 12:31:00 July 12 2004.
config-register *valor_registro_configuración*	Cambia los valores del registro de configuración. Ejemplo: config-register 0x2142.
enable password *contraseña*	Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio. Ejemplo: enable password class.
enable secret *contraseña*	Especifica una capa de seguridad adicional mediante el comando enable password. Ejemplo: enable secret class.
hostname *nombre*	Modifica el nombre del router. Ejemplo: hostname Lab_A.
interface *tipo número*	Configura un tipo de interfaz y entra al modo de configuración de interfaz. Ejemplo: interface ethernet 0.
ip access-list {tandard|extended} *Nombre*	Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router en el submodo de configuración que puede reconocerse por el prompt. Router(config-ext-nacl)#
ip classless	Evita que el router tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto.
ip default-network *dirección_red*	Establece una ruta por defecto. Ej.: ip default-network 210.32.45.0
ip domain-lookup	Habilita la conversión de nombre a dirección en el router.
ip host *nombre_host dir_ip1 …. Dir_ip8*	Crea una entrada de nombre a dirección estática en el archivo de configuración del router. Ej.: ip host Lab_A 192.168.5.1 210.110.11.1
ip http server	Permite que el router actúe como servidor web http limitado.
ip name-server *dir_ip1 …. Dirip6*	Especifica las direcciones de hasta seis servidores de nombre para su uso en la resolución de nombres y direcciones.
Ip route *dirección_red máscara dir_ip_salto* [*distancia_administrativa*]	Establece rutas estáticas. Ejemplo: ip route 210.42.3.0 255.255.255.0 211.1.2.1
line *tipo número*	Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración. Ej.: line console 0 *ó* line vty 0 4.
router *protocolo_de_enrutamiento* [*nro_AS*]	Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ejemplo: router rip *ó* router igrp 120.
service password-encryption	Habilita la función de cifrado de la contraseña.

SUBMODO DE CONFIGURACIÓN DE INTERFAZ

Comando	Descripción
bandwidth *Kbps*	Establece un valor de ancho de banda para una interfaz. Ejemplo: bandwidth 64.
cdp enable	Habilita Cisco Discovery Protocol en una interfaz.
cdp holdtime *segundos*	Especifica el tiempo de espera antes de ser enviada la siguiente actualización CDP.
cdp timer *segundos*	Especifica la frecuencia con que son enviadas las actualizaciones CDP.
clock rate *velocidad*	Configura la velocidad de reloj para las conexiones de hardware en interfaces seriales, como módulos de interfaz de red y procesadores de interfaz a una velocidad de bits aceptable. Ejemplo: clock rate 56000.
description *descripción*	Agrega una descripción a la interfaz. Ejemplo: description Conectada a Internet.
ip access-group *Nro_ACL* [in|out]	Asigna la ACL indicada a la interfaz, ya sea para que verifique los paquetes entrantes (in) o los salientes (out).
ip address *dirección_ip mascara_red*	Asigna una dirección y una máscara de subred, e inicia el procesamiento IP en una interfaz. Ejemplo: ip address 192.168.52.1 255.255.255.0
no ip route-cache	Para deshabilitar el balanceo de carga por destino que esté habilitado por defecto.
no ip split-horizon	Deshabilita el horizonte dividido en la interfaz, que por defecto se encuentra habilitado. Para volver a habilitarlo utilice el comando ip split-horizon.
no shutdown	Reinicia una interfaz desactivada.
shutdown	Inhabilita una interfaz.

SUBMODO DE CONFIGURACIÓN DE LINEA

Comando	Descripción
access-class *Nro_ACL* in	En las líneas VTY, asigna una lista de control de acceso a las conexiones establecidas vía Telnet.
login	Habilita la verificación de contraseña en el momento de la conexión.
password *contraseña*	Asigna la contraseña a ser solicitada en el momento de la conexión.

- **SUBMODO DE CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO**

Comando	Descripción
maximum-paths *valor*	Permite modificar el máximo de rutas sobre las que balanceará la carga.
metric weights *tos k1 k2 k3 k4 k5*	Permite modificar los valores de las constantes utilizadas para el cálculo de las métricas de las rutas en el protocolo de enrutamiento IGRP. Los valores por defecto son: *tos* (tipo de servicio)= 0; *k1*= 1; *k2*= 0; *k3*= 1; *k4*= 0 y *k5*= 0.
neighbor *dirección_ip*	Como RIP es un protocolo de tipo broadcast, el administrador de la red podría tener que configurarlo para que intercambie información de enrutamiento en redes no broadcast, como en el caso de las redes Frame Relay. En este tipo de redes, RIP necesita ser informado de otros routers RIP vecinos.
network *dirección_red*	Asigna una dirección de red a la cual el router se encuentra directamente conectado, lo que hará que se envíen y reciban publicaciones de enrutamiento a través de esa interfaz, además de que sea publicada a los routers vecinos. Ejemplo: network 210.45.2.0
no timers basic	Regresa los temporizadores a los valores por defecto.
passive-interface *tipo número*	El router no enviará información de enrutamiento por la interfaz indicada. Ejemplo: passive-interface serial 0.
redistribute static	Si se asigna una ruta estática a una interfaz que no está definida en el proceso RIP o IGRP, mediante el comando network, no será publicada la ruta a menos que se especifique este comando.
timers basic *Actualización Inválida Espera Purga* [*Suspensión*]	Indica la frecuencia con la que RIP o IGRP envían actualizaciones y los intervalos de los temporizadores. *Actualización:* intervalo en segundos al que se envían las actualizaciones (RIP: 30''; IGRP: 90''). *Inválida:* Intervalo de tiempo en segundos después del cual una ruta se declara no válida. Sin embargo, la ruta todavía se utiliza para el envío de paquetes (RIP: 180''; IGRP: 270''). *Espera:* Intervalo en segundos durante el cual se suprime la información de enrutamiento referida a las mejores rutas (RIP: 180''; IGRP: 280''). *Purga:* Intervalo de tiempo en segundos que debe transcurrir antes de que la ruta se elimine de la tabla de enrutamiento (RIP: 240''; IGRP: 630''). *Suspensión:* Intervalo en milisegundos en que se posponen las actualizaciones de enrutamiento cuando se produce una actualización Flash. Sólo IGRP.
variance *valor*	El valor de variación determina si IGRP aceptará rutas de costo desigual. Sólo aceptará rutas iguales a la mejor métrica local para el destino multiplicado por el *Valor* de variación. El *valor* puede variar de 1 (por defecto) a 128.

COMANDOS DE EDICIÓN y OTROS

Teclas / Comando	Descripción
Ctrl+A	Permite desplazarse al principio de la línea de comandos.
Esc+B	Permite desplazarse una palabra hacia atrás.
Ctrl+B (o flecha izquierda)	Permite desplazarse un carácter hacia atrás.
Ctrl+E	Permite desplazarse hasta el final de la línea de comandos.
Ctrl+F (o flecha derecha)	Permite desplazarse un carácter hacia adelante.
Ctrl+P (o flecha arriba)	Muestra el último comando ingresado.
Ctrl+N (o flecha abajo)	Muestra el comando más reciente.
<Tab> (tecla tabulador)	Completa el comando ingresado parcialmente.
Ctrl+Z (o end)	Estando en cualquier modo de configuración, regresa al modo EXEC Privilegiado.
Ctrl+C	Cancela la ejecución del *Diálogo de configuración inicial* o *Setup*.
Ctrl+Shift+6	Permite interrumpir intentos de ping, traceroute y traducciones de nombres.
Exit	Estando en el modo de configuración global o cualquiera de sus submodos, regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión.

VIII. SOFTWARE

1. SNIFFER

Un sniffer es un programa de captura de las tramas de red. Es algo común que el medio de transmisión (cable coaxial, UTP, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguirlo, el sniffer le dice a la computadora que deje de ignorar todo el tráfico no destinado al equipo y le ponga atención. Esto es conocido como poner en estado *promiscuo* a la NIC (Network Interface Card).

En la actualidad, la seguridad en las redes es de vital importancia, ya que toda la información que se transmite a través de éstas muchas veces puede ser utilizada para fines de lucro o perpetrar delitos electrónicos.

Una vez que la NIC se encuentra en este estado se necesitarán los privilegios administrativos o de root, de esta manera la computadora será capaz de ver todos los datos transmitidos. Es entonces cuando el programa comienza a hacer una lectura de toda la información entrante a la PC por la tarjeta de red. Con esto, el sniffer conseguirá observar el equipo de origen, el equipo de destino, el número de puerto, etc. En resumen, podrá ver la información intercambiada entre dos computadoras.

El uso que se dé a este tipo de aplicaciones es algo importante de señalar, ya que gracias a ellas podemos colaborar con que nuestra red tenga más seguridad, hacer pruebas y así poder tener un muy buen resultado, el problema viene cuando otros usuarios las utilizan con fines de delitos electrónicos, ya que con este tipo de herramientas se puede obtener información confidencial.

Los principales usos que se les puede dar son:

- Captura de contraseñas enviadas sin cifrar y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por atacantes ("hackers") para atacar sistemas.
- Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- Para los desarrolladores, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red.

Algunos sniffers trabajan sólo con paquetes de TCP/IP, pero hay otros más sofisticados que son capaces de trabajar con un número más amplio de protocolos e incluso en niveles más bajos, como el de las tramas del Ethernet. Entre los más utilizados tenemos los siguientes:

- Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.2 Broadcast ARP Who has 192.168.0.2? Gratuitous
2 0.299139 192.168.0.1 192.168.0.2 NBNS Name query NBSTAT
3 0.299214 192.168.0.2 192.168.0.1 ICMP Destination unreachable (Port
4 1.025459 192.168.0.2 224.0.0.22 IGMP V3 Membership Report
5 1.044166 192.168.0.2 192.168.0.1 DNS Standard query SRV _ldap._tcp.nbg
6 1.044643 192.168.0.2 239.255.255.250 UDP Source port: 3183 Destination
7 1.055784 192.168.0.2 192.168.0.1 DNS Standard query SOA nb100410.wm004
8 1.055853 192.168.0.1 192.168.0.2 UDP Source port: 1900 Destination
9 1.063034 192.168.0.2 192.168.0.255 NBNS Registration NB NB100410<00>
10 1.111345 192.168.0.2 192.168.0.1 DNS Standard query A proxyconf.wm004
11 [illegible]
12 1.207282 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack=
Frame 11 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:09:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
Source port: 3196 (3196)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
Window size: 64240

- Ettercap es un interceptor/sniffer/registrador para las Lan con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso de aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo, aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo.
- Kismet es un sniffer, un husmeador de paquetes y un sistema de detección de intrusiones para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante y compatible de paquetes es otra sonda.
- TCPDUMP es un herramienta de comandos en línea cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

Un sniffer puede ser de gran utilidad en la administración de una red, con fines de seguridad y funcionalidad, pero hay que tomar en cuenta que es una herramienta que puede ser de doble filo, ya que algún usuario puede utilizarla con un fin inadecuado y pueda tomar ventaja de esto. Es importante conocer el funcionamiento de estas aplicaciones para que en un caso dado podamos utilizarlas en determinadas circunstancias.

2. HERRAMIENTAS CISCO

SDM (Security Device Manager)

SDM es una herramienta de mantenimiento con una interfaz web basada en Java y desarrollada por Cisco. Es soportada por un amplio número de routers Cisco IOS. En la actualidad se entrega preinstalada en la mayoría de los routers nuevos de Cisco.

Para acceder a la herramienta hay dos formas:

1. Si está instalada en el ordenador, seleccione el icono de SDM. Se abrirá una ventana de diálogo requiriendo el ingreso de la dirección IP del dispositivo. Ingrese la IP del dispositivo e inmediatamente se abrirá una ventana del navegador para comenzar el proceso de carga.
2. Si desea acceder desde el router directamente, abra una ventana del navegador de Internet y escriba en la barra de direcciones la dirección IP del dispositivo al que desea acceder.

En principio ofrece una pantalla inicial para monitorear el estado del dispositivo.

Respecto de las opciones de configuración que ofrece, son extremadamente amplias y van desde la configuración básica del dispositivo Firewall hasta servicios como DHCP, NAT, VPN, etc.

ACS (Access Control Server)

Cisco ACS es un servidor de autenticación basado en RADIUS, capaz de compartir datos sobre cuentas de usuarios finales, plataforma para la auditoría de cuentas de usuarios, creación de políticas ACS, entre otras cosas.

Esto facilita a los clientes la sincronización entre políticas de seguridad de usuario y datos a través del hardware de Cisco, y las plataformas de seguridad basadas en software de otros fabricantes. La integración podría incluir a todos los routers, conmutadores y sistemas VPN de Cisco gestionados por ACS, así como a las aplicaciones de software.

Cisco Secure ACS proporciona una interfaz de administración web conocido como CSAdmin, activa en el puerto 2002. Cuando se rebosa de conexiones TCP, el ACS Windows y ACS Solution Engine dejan de responder a cualquier nueva conexión TCP destinada al puerto 2002.

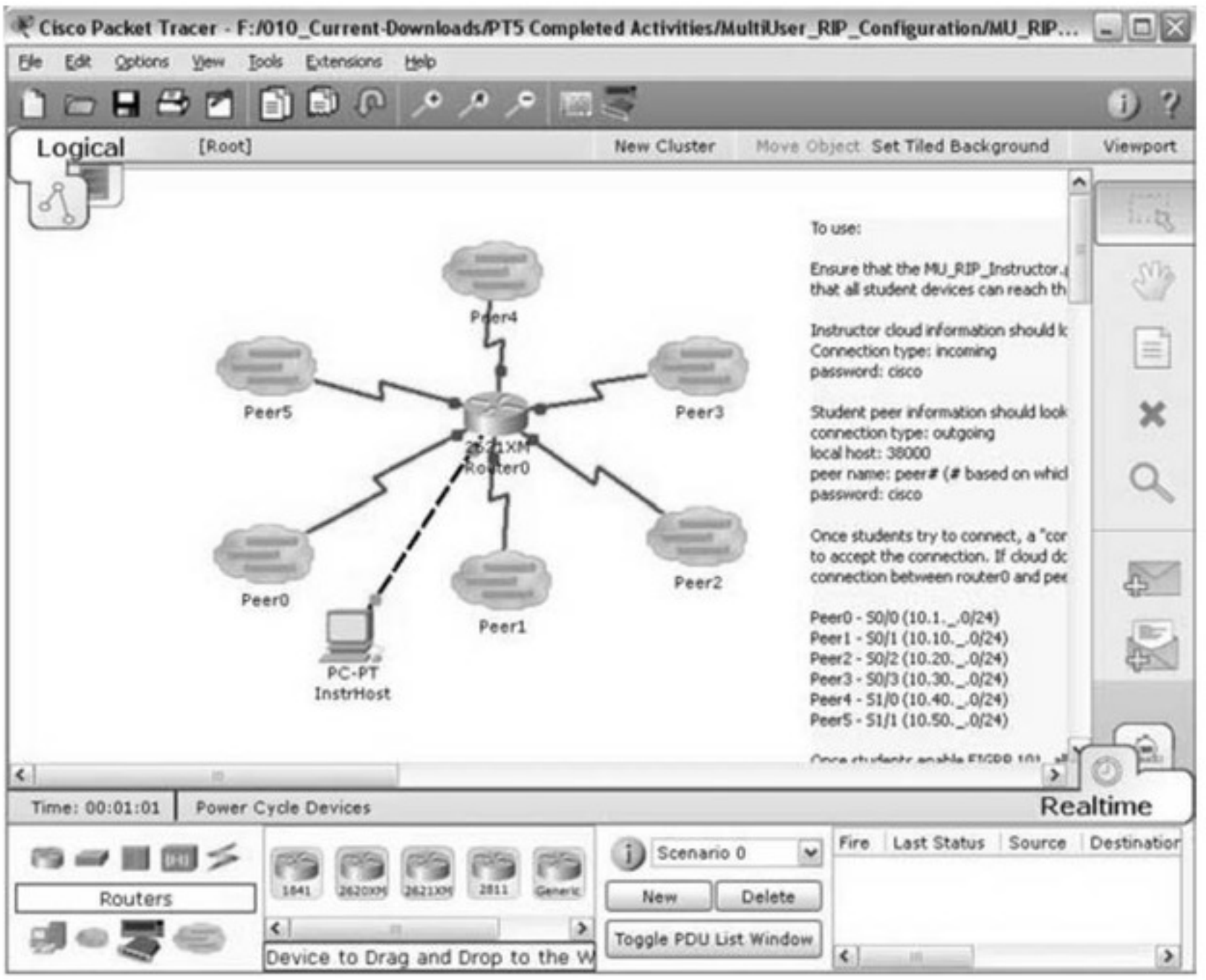
CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1:1107/
Google
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows
Cisco Systems
Cisco Secure ACS v4.0
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Log Off
Select "Log Off" to end the administration session.
CiscoSecure ACS v4.0 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.
CiscoSecure ACS
Release 4.0(1) Build 27
Copyright ©2005 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3. SIMULADORES Y EMULADORES

La principal diferencia entre un emulador y un simulador es que con el emulador usamos el software IOS real de un router y, por lo tanto, prácticamente todo lo que se pueda configurar con ese IOS lo podemos hacer con el emulador.

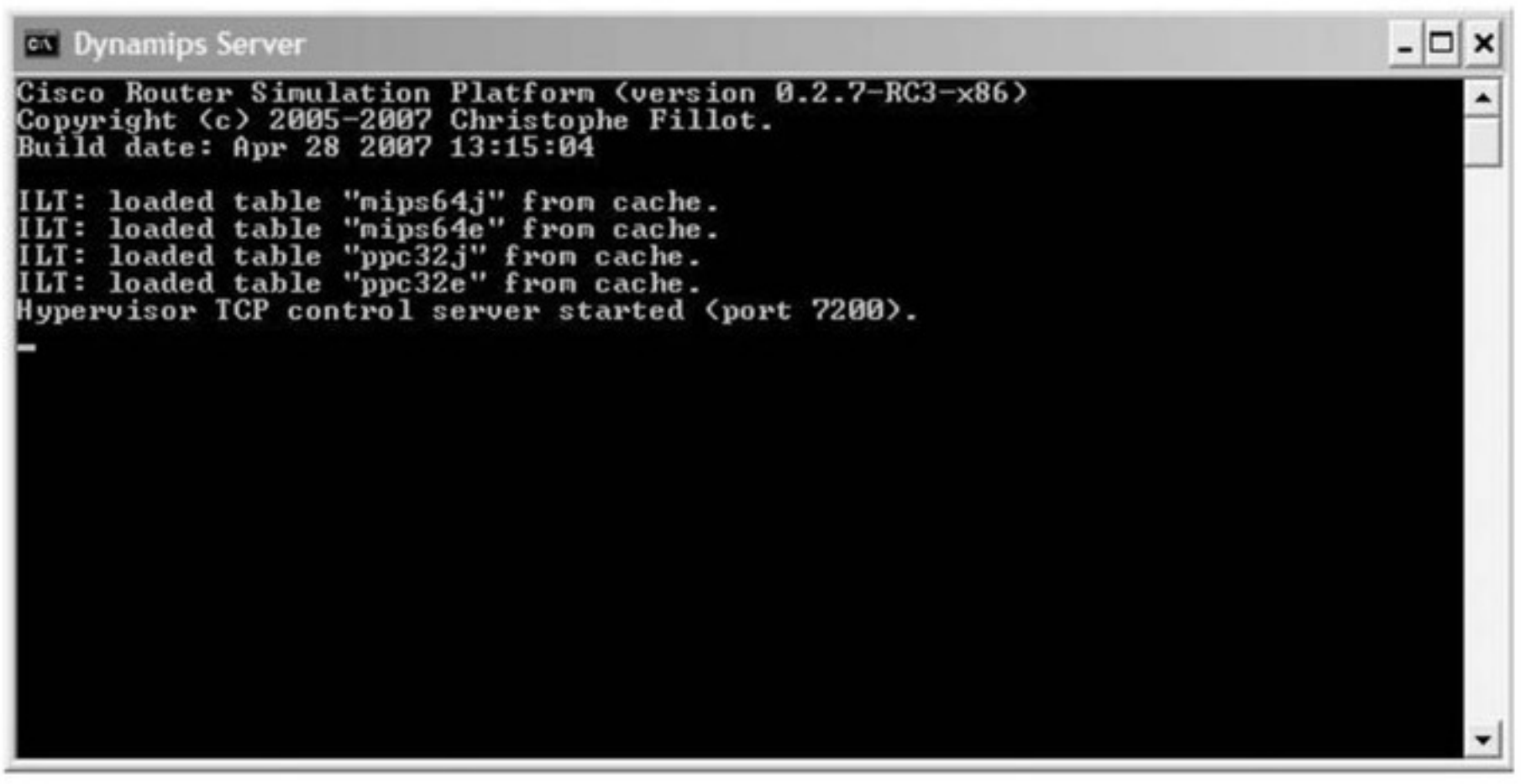
PACKET TRACER

Es una herramienta de aprendizaje y simulación de redes interactivas para toda persona que quiera comenzar a estudiar o instruirse en los fundamentos de redes y principalmente en las certificaciones de Cisco. Esta herramienta educativa permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. También permite una exposición a la interfaz Comando en línea, de los dispositivos de Cisco, para practicar y aprender por descubrimiento.



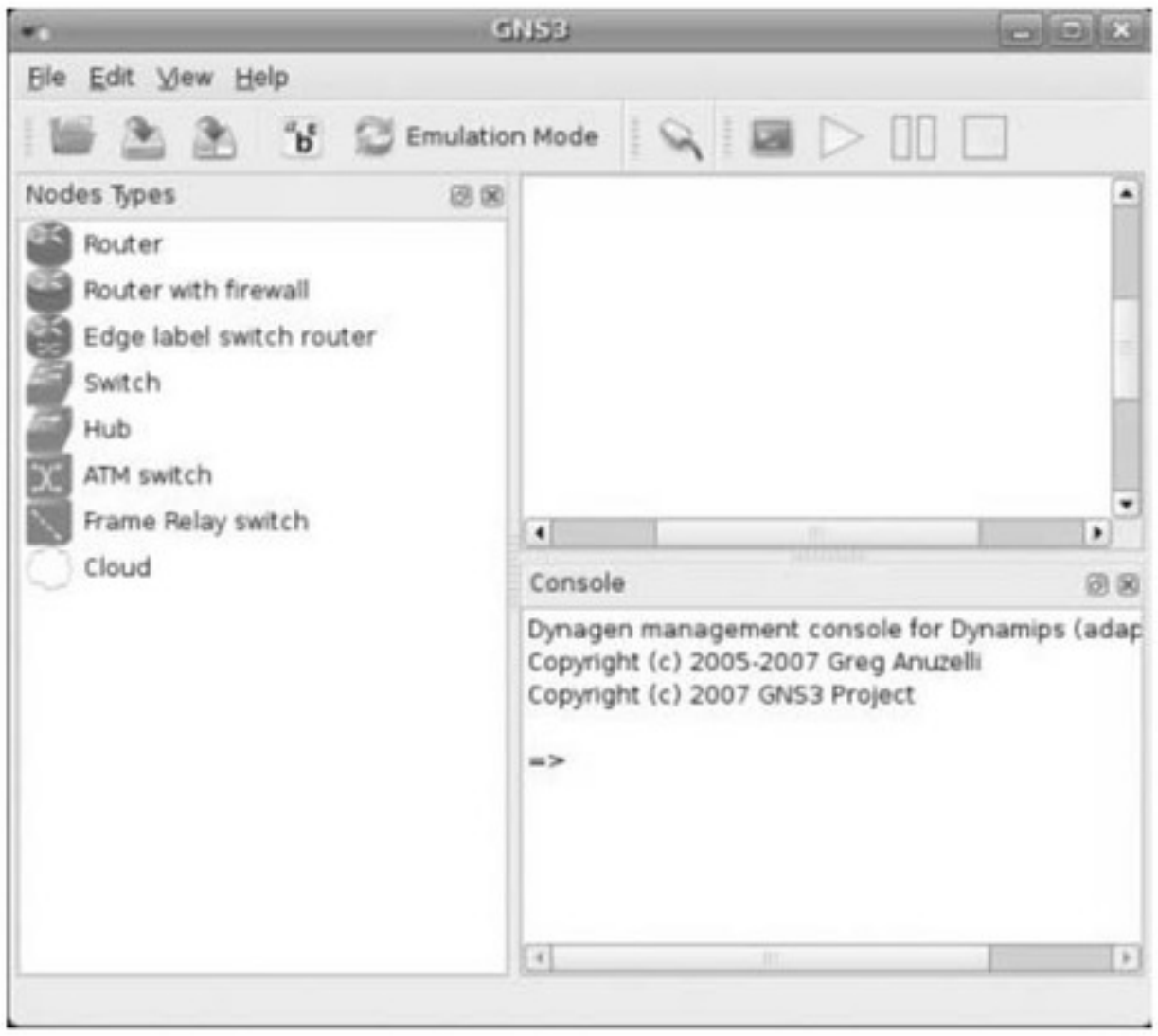
DYNAMIPS

Este programa permite emular el software que es ejecutado en los ruteadores Cisco y esto es especialmente útil pues ningún emulador proporciona los comandos completos del software Cisco IOS. Se presenta en un entorno de consola de comandos para Windows y Linux. Más información respecto a dynamips en http://www.dynagen.org/.


Dynamips Server
Cisco Router Simulation Platform (version 0.2.7-RC3-x86)
Copyright (c) 2005-2007 Christophe Fillot.
Build date: Apr 28 2007 13:15:04
ILT: loaded table "mips64j" from cache.
ILT: loaded table "mips64e" from cache.
ILT: loaded table "ppc32j" from cache.
ILT: loaded table "ppc32e" from cache.
Hypervisor TCP control server started (port 7200).

GNS3

Usamos el emulador GNS3 basado en el software Dynamips. Este software nos permite hacer una emulación casi perfecta de un ambiente con routers Cisco series 1700, 2600, 3600, 3700 y 7200. Se presenta en un entorno de consola gráfica **para Windows y Linux**. Más información respecto al trabajo de este programa puede encontrarse en http://www.gns3.net/.



4. OTROS PROGRAMAS:

HYPERTERMINAL

HyperTerminal es un programa que se puede utilizar para conectar con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS), servicios en línea y equipos host. Las conexiones se realizan mediante un módem, un cable de módem nulo (utilizado para emular la comunicación por módem) o una conexión Ethernet.

HyperTerminal tiene capacidades que van más allá del establecimiento de conexiones con otros equipos. Puede, por ejemplo, transferir archivos grandes de un equipo a un equipo portátil a través del puerto serie, en lugar de requerir la configuración del equipo portátil en una red. También puede ayudar a depurar el código fuente desde un terminal remoto. Además, puede establecer una comunicación con los equipos antiguos basados en caracteres.

Network Inspector™

Network Inspector es una solución que realiza un seguimiento y diagnostica de forma activa los problemas en entornos TCP/IP, IPX y NetBIOS. Network Inspector, diseñado para redes Ethernet Lan, identifica rápidamente si el problema se encuentra en un servidor, cliente, conmutador, enrutador o impresora, gracias a la rápida detección y clara visualización de la red. Está diseñado con un agente de seguimiento y una arquitectura de consola de visualización. Los agentes pueden distribuirse en la red, de forma tal que cada uno realice un seguimiento de un dominio de difusión y que una o varias consolas tengan acceso remoto a los datos recopilados por dichos agentes.

PComm Lite, PODEROSA y TN3270

Son herramientas de emulación similares al HyperTerminal que permiten el acceso a la administración de equipos mediante el puerto consola.

TFTP

Es siempre necesario el empleo de software de servidores TFTP que faciliten la configuración del equipo para la transferencia de archivos de respaldo.

Kiwi Syslog Daemon

Es un demonio del syslog para la plataforma de Windows. Recibe y registra las exhibiciones, y remite mensajes del syslog de los anfitriones tales como router, switch, servidores de Unix y cualquier otro dispositivo syslog permitido. Hay muchas opciones mejoradas disponibles. Las características incluyen: PIX, cortafuegos que registra, trampa del SNMP, ayuda del TCP, MIB que analiza, filtro de LinkSys.

Bibliografía

- Cisco Networking Academy. Certification CCNA, Exploration Version 4.0.
- Cisco Networking Academy. Certification CCNA, Version 3.1.
- Dye, Mark; Rick McDonald and Antoon Rufi. Network Fundamentals, CCNA Exploration Companion Guide (Nov 8, 2007).
- Graziani, Rick and Allan Johnson. Routing Protocols and Concepts, CCNA Exploration Companion Guide (Dec 16, 2007).
- Graziani, Rick and Bob Vachon. Accessing the WAN, CCNA Exploration Companion Guide (May 8, 2008).
- Lewis, Wayne. LAN Switching and Wireless, CCNA Exploration Companion Guide (May 8, 2008).
- Teare, Diane and Catherine Paquet. Building Scalable Cisco Internetworks (BSCI). Authorized Self-Study Guide, 3rd edition (Jan 5, 2007).

Impreso en los Talleres Gráficos de

EMPRESA EDITORA MACRO®

Surquillo

☎ 243-2003 – 827*2650

Octubre 2009